SonicWALL Internet Security Appliances

SonicWALL SSL VPN 3.5 User's Guide

SONICWALL®

Table of Contents

Using This Guide

About this Guide 5
Organization of this Guide 5
Guide Conventions 5
Icons Used in this Manual 6
Current Documentation 7
Important Information You Need 7

Virtual Office Overview

Virtual Office Overview 9
Accessing Virtual Office Resources 9
Browser Requirements 11
Web Management Interface Overview 12
Certificates 15

Using Virtual Office Features

Importing Certificates 17
Using Two-Factor Authentication 18
User Prerequisites 18
User Configuration Tasks 18
Using One-Time Passwords 21
User Prerequisites 21
User Configuration Tasks 21
Verifying User One-Time Password Configuration 23
Troubleshooting Common Errors 23
Using NetExtender 23
User Prerequisites 23
User Configuration Tasks 24

Related Documents 56
Using Virtual Assist 56
Launching a Virtual Assist Technician Session 57
Performing Virtual Assist Technician Tasks 61
Using Virtual Assist from the Customer View 65
Using File Shares 70
Using the File Shares Applet 71
Using HTML-Based File Shares 84
Managing Bookmarks 87
Adding Bookmarks 88
Editing Bookmarks 92
Removing Bookmarks 93
Using Bookmarks 93
Using Remote Desktop Bookmarks 93
Using VNC Bookmarks 95
Using FTP Bookmarks 98
Using Telnet Bookmarks 101
Using SSHv1 Bookmarks 102
Using SSHv2 Bookmarks 103
Using HTTP and HTTPS Bookmarks 104
Using File Share Bookmarks 105
Using Citrix Bookmarks 105
Global Bookmark Single Sign-On Options 108
Per-Bookmark Single Sign-On Options 108
Logging Out of the Virtual Office 110
Trademarks 110
Limited Warranty 110

Using This Guide

About this Guide

Welcome to the *SonicWALL SSL VPN User's Guide*. This manual is a user's guide. It provides information on using the SonicWALL SSL VPN user portal called Virtual Office that allows you to create bookmarks and run services over the SonicWALL SSL-VPN security appliance.

Note Always check http://www.sonicwall.com/us/Support.html for the latest version of this manual as well as other SonicWALL products and services documentation.

Organization of this Guide

The *SonicWALL SSL VPN User's Guide* organization is structured into the following parts:

Chapter 1 Virtual Office Overview

This chapter provides an overview of new SonicWALL SSL-VPN security appliance user features, NetExtender, File Shares, services, sessions, bookmarks, and service tray menu options.

Chapter 2 Using Virtual Office

This chapter provides procedures on how to install NetExtender, working with the NetExtender system tray, displaying the NetExtender log, configuring bookmarks, and using file shares.

Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Also, sometimes indicates the first instance of a significant term or concept.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

Tip Useful information about security features and configurations on your SonicWALL.

Note Important information on a feature that requires callout for special attention.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at http://www.sonicwall.com/us/Support.html. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1.408.752.7819

International Telephone Support

Australia - + 1.800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39(0)2.7541.9803

Japan - +81 (0) 3-3457-8971

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41(0)1.308.3.977

UK - +44(0)1344.668.484

Note Please visit http://www.sonicwall.com/us/support/contact.html for the latest technical support telephone numbers.

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
Email: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408)745-9300

Current Documentation

Check the SonicWALL documentation Web site for the latest versions of all SonicWALL product documentation at http://www.sonicwall.com/us/Support.html

Quick Access Work Sheet

This section should be completed by your network administrator to allow remote users SSL VPN access.

Important Information You Need

IP Address:_____

User Name:_____

Password:_____

Domain:_____

Virtual Office Overview

This chapter provides an overview of the SonicWALL SSL VPN user portal. It also includes an introduction to the SSL-VPN and its features and applications. This chapter contains the following sections:

- "Virtual Office Overview" section on page 9
- "Browser Requirements" section on page 11
- "Web Management Interface Overview" section on page 12

Virtual Office Overview

SonicWALL SSL VPN Virtual Office provides secure remote access to network resources, such as applications, files, intranet Web sites, and email through Web access interface such as Microsoft Outlook Web Access (OWA). The underlying protocol used for these sessions is SSL.

With SSL VPN, mobile workers, telecommuters, partners, and customers can access information and applications on your intranet or extranet. What information should be accessible to the user is determined by access policies configured by the SonicWALL SSL VPN administrator.

Accessing Virtual Office Resources

Remote network resources can be accessed in the following ways:

- **Using a standard Web browser** - To access network resources, you must log into the SSL VPN portal. Once authenticated, you may access intranet HTTP and HTTPS sites, Web-based applications, and Web-based email. In addition, you may upload and download files using FTP or Windows Network File Sharing. All access is performed through a standard Web browser and does not require any client applications to be downloaded to remote users' machines.
- **Using Java thin-client access to corporate desktops and applications** – The SonicWALL SSL-VPN security appliance includes several Java or ActiveX thin-client programs that can be launched from within the SonicWALL SSL-VPN security appliance. Terminal Services and VNC Java clients allow remote users to access corporate servers and desktops, open files, edit and store data as if they were at the office. Terminal Services provides the ability to open individual applications and support remote sound and print services. In addition, users may access Telnet and SSH servers for SSH version 1 (SSHv1) and SSH version 2 (SSHv2), from the SSL VPN portal.

- **Using the NetExtender SSL VPN client** – The SonicWALL SSL VPN network extension client, NetExtender, is available through the SSL VPN Virtual Office portal via an ActiveX control or through stand-alone applications for Windows, Linux, and MacOS platforms. To connect using the SSL VPN client, log into the portal, download the installer application and then launch the NetExtender connector to establish the SSL VPN tunnel. Once you have set up the SSL VPN tunnel, you can access network resources as if you were on the local network.

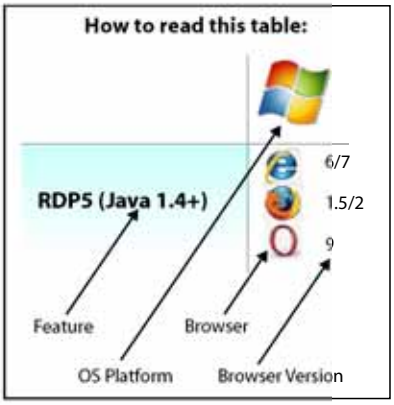
  The NetExtender standalone applications are automatically installed on a client system the first time you click on the NetExtender link in the Virtual Office portal. The standalone client can be launched directly from users' computers without requiring them to log in to the SSL VPN portal first.

For SSL VPN to work as described in this guide, the SonicWALL SSL-VPN security appliance must be installed and configured according to the directions provided in the *SonicWALL SSL-VPN Getting Started Guide* for your model.

Browser Requirements

The following Web browsers are supported for the SSL VPN portal. features. For administrator portal Web browser compatibility, refer to the SonicWALL SSL VPN Administrator's Guide.

Application Proxy Minimum Browser/Version Requirements				
NetExtender	6, 7 1.5/2	7 1.5/2	browser independent (Java 1.4+)	browser independent (Java 1.4+)
RDP5 (ActiveX)	6/7	7		
RDP5 (Java 1.4+)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2 9	2 1.5/2
VNC (Java 1.1+)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2 9	2 1.5/2 9
Telnet (Java 1.1+)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2	2 1.5/2 9[4]
SSHv1, SSHv2 (Java 1.4+)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2	2 1.5/2 9[4]
HTTP, HTTPS, FTP (Browser)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2 9	2 1/1.5/2 9
File Sharing (Browser)	6/7 1/1.5/2 9	7 1/1.5/2 9	1/1.5/2 9	2 1/1.5/2 9[3]
File Sharing (Java 1.2+)	6/7 1/1.5/2 9[2]	7 1/1.5/2 9[2]	1/1.5/2 9[2]	2 1.5/2
Citrix (ActiveX)	6/7			
Citrix (Java 1.4+)	6/7 1/1.5/2 9[6]	7 1/1.5/2 9[6]	1/1.5/2	2 1.5/2
Virtual Assist (Java not required)	6/7 2 9	7 2 9		



Notes:

* Firefox 1.0 may truncate long lists of bookmarks on the Virtual Office portal.

2 Remote window starts out collapsed and must be manually resized.

4 Telnet/SSH applets under Mac Opera may have keyboard focus issues.

5 Popups must be enabled under Site Preferences (for authentication windows).

6 MetaFrameXP FR3 works, Presentation Server 4 Login screen is not accessible.

To configure SonicWALL SSL VPN firmware, an administrator must use a Web browser with JavaScript, cookies, and SSL enabled.

Before using Virtual Assist, you must meet the following requirements:

- Virtual Assist is only supported on the SonicWALL SSL-VPN 2000, SSL-VPN 4000, and SRA 4200 platforms.
- Virtual Assist is only supported on Windows platforms. Virtual Assist is certified to work on Windows XP and Windows 2000.

Web Management Interface Overview

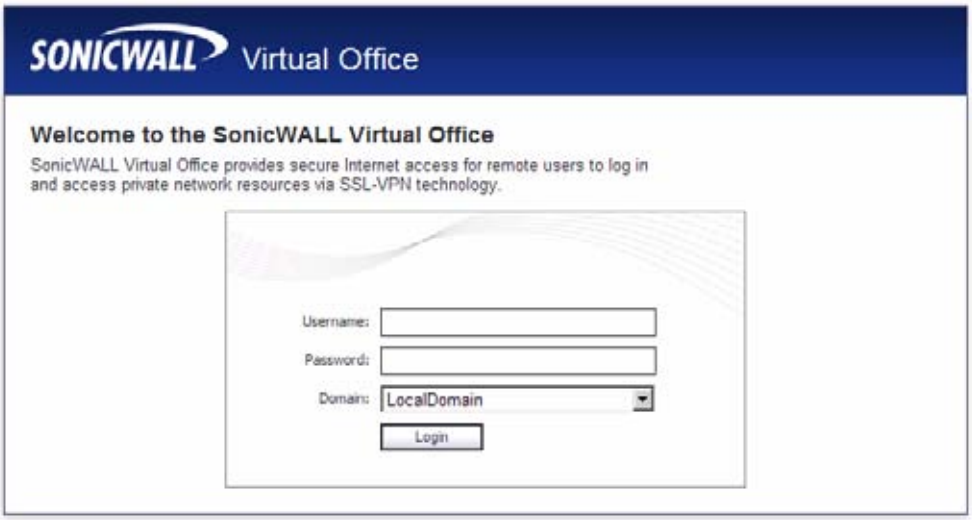
From your workstation at your remote location, launch an approved Web browser and browse to your SSL-VPN appliance at the URL provided to you by your network administrator.

Step 1 Open a Web browser and enter **https://192.168.200.1** (the default LAN management IP address) in the **Location** or **Address** field.

Step 2 A security warning may appear. Click the **Yes** button to continue.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

Step 3 The **SonicWALL SSL VPN Management Interface** displays and prompts you to enter your user name and password. As a default value, enter **admin** in the **User Name** field, **password** in the **Password** field, and select a domain from the **Domain** drop-down list and click the **Login** button. Only **LocalDomain** allows administrator privileges. Note that your administrator may have set up another login and password for you that has only user privileges.


SONICWALL Virtual Office
Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Username:
Password:
Domain:
LocalDomain
Login

The default page displayed is the Virtual Office home page. The default version of this page shows a SonicWALL logo, although your company's system administrator may have customized this page to contain a logo and look and feel of your company. Go to the Virtual Office Overview, page 9 to learn more about the Virtual Office home page.

Note From the Virtual Office portal home page, you cannot navigate to the administrator's environment. If you have administrator's privileges and want to enter the administrator environment, you need to go back to the login page and enter a username and password that have administrator privileges, and login again using the LocalDomain domain. Only the LocalDomain allows administrator access to the management interface. Also note that the domain is independent of the privileges set up for the user.

Logging in as a user takes you directly to Virtual Office. The Virtual Office Home page displays as shown here.

SONICWALL Virtual Office
User: jpollock
Session Status: Active
Options
Help
Logout
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Virtual Assist
Assist someone by taking control of their computer.
All Bookmarks
Desktop
Web
Files
Show Edit Controls
Agile
Product Lifecycle Management
Citrix to home
Citrix (HTTPS)
DFS
Distributed File System
NDConnector
Terminal Services (RDP - ActiveX)
Webmail
SonicWALL Webmail
Tips/Help
Search Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.
What is Virtual Assist?
Virtual Assist allows you to remotely support customers by taking control of their computers while the customer observes.
How can I add more bookmarks?
Click "Show Edit Controls" (above the bookmark table, toward the right-hand side), then click "New Bookmark". If either of these options are missing, your administrator may not have given you permission to add bookmarks.

Note The Virtual Office content will vary based on the configuration of your network administrator. Some bookmarks and services described in the *SonicWALL SSL VPN User's Guide* may not be displayed when you log into the SonicWALL SSL-VPN security appliance.

The Virtual Office consists of the nodes described in the following table.

Node	Description
File Shares	Provides access to the File Shares utility, which gives remote users with a secure Web interface access to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.
NetExtender	Provides access to the NetExtender utility, a transparent SSL VPN client for Windows, MacOS, or Linux users that allows you to run any application securely on the remote network. It acts as an IP-level mechanism provided by the virtual interface that negotiates the ActiveX component (on Windows with IE), using a Point-to-Point Protocol (PPP) adapter instance. On non-Windows platforms, Java controls are used to automatically install NetExtender from the Virtual Office portal. After installation, NetExtender automatically launches and connects a virtual adapter for SSL secure NetExtender point-to-point access to permitted hosts and subnets on the internal network.
Virtual Assist (SSL-VPN 2000 / SSL-VPN 4000 / SRA 4200 only)	Provides access to Virtual Assist, an easy to use tool that allows SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Virtual Assist is a lightweight, thin client that installs automatically using Java from the SonicWALL SSL VPN Virtual Office without requiring the installation of any external software. For computers that do not support Java, Virtual Assist can be manually installed by downloading an executable file from the Virtual Office.
Bookmarks	Provides a list of available bookmarks which are objects that enable you to connect to a location or application conveniently and quickly.
Options	Provides the option to change user password and use single sign-on, if enabled by the administrator.
Online Help	Launches online help for Virtual Office.
Tips/Help	Provides a short list of common questions and tips about the Virtual Office.
Logout	Logs you out of the Virtual Office environment.

The Home page provides customized content and links to network resources. The Home Page may contain support contact information, VPN instructions, company news, or technical updates.

Only a Web browser is required to access intranet Web sites, File Shares, and FTP sites. VNC, Telnet and SSHv1 require Java. SSHv2 provides stronger encryption than SSHv1, requires SUN JRE 1.4 or above and can only connect to servers that support SSHv2. Terminal Services requires either Java or ActiveX on the client machine.

As examples of tasks you can perform and environments you can reach through Virtual Office, you can connect to:

- Intranet Web or HTTPS sites – If your organization supports Web-based email, such as Outlook Web Access, you can also access Web-based email
- The entire network by launching the NetExtender client
- FTP servers for uploading and downloading files
- The corporate network neighborhood for file sharing
- Telnet and SSH servers
- Desktops and desktop applications using Terminal Services or VNC.
- Email servers via the NetExtender client.

The administrator determines what resources are available to users from the SonicWALL SSL VPN Virtual Office. The administrator can create user, group, and global policies that disable access to certain machines or applications on the corporate network.

The administrator may also define bookmarks, or preconfigured links, to Web sites or computers on the intranet. Additional bookmarks may be defined by the end user.

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

Certificates

If the SSL-VPN appliance uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Using Virtual Office Features

This chapter provides details on how to use the features in the SonicWALL SSL VPN user portal, including NetExtender, configuring bookmarks, accessing services, and using file shares. This chapter contains the following sections:

- "Importing Certificates" section on page 17
- "Using Two-Factor Authentication" section on page 18
- "Using One-Time Passwords" section on page 21
- "Using NetExtender" section on page 23
- "Using Virtual Assist" section on page 56
- "Using File Shares" section on page 70
- "Managing Bookmarks" section on page 87
- "Using Bookmarks" section on page 93
- "Logging Out of the Virtual Office" section on page 110

Importing Certificates

If the SSL VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate.

The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page. The following warning messages may be displayed:

Click **Yes**. The certificate will be imported.

Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

Using Two-Factor Authentication

The following sections describe how to log in to the SSL VPN Virtual Office portal using two-factor authentication:

- "User Prerequisites" on page 18
- "User Configuration Tasks" on page 18

User Prerequisites

Before you can log in using two-factor authentication, you must meet the following prerequisites:

- Your administrator has created your user account.
- You have either an RSA SecurID token or a VASCO Digipass token.

User Configuration Tasks

The following sections describe how users log in to the SonicWALL SSL-VPN appliance using the two types of two-factor authentication:

- "RSA User Authentication Process" on page 18
- "VASCO User Authentication Process" on page 20

RSA User Authentication Process

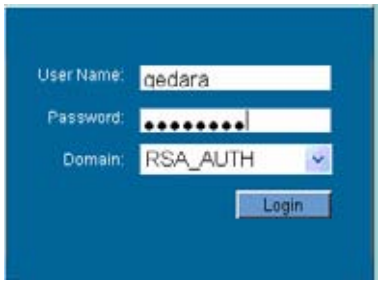
The following sections describe user tasks when using RSA two-factor authentication to log in to the SonicWALL SSL VPN Virtual Office:

- "Logging into the SSL VPN Virtual Office Using RSA Two-Factor Authentication" on page 18
- "Creating a New PIN" on page 19
- "Waiting for the Next Token Mode" on page 20

Logging into the SSL VPN Virtual Office Using RSA Two-Factor Authentication

To log in to the SonicWALL SSL VPN Virtual Office using RSA two-factor authentication, perform the following steps.

Step 1 Enter the IP address of the SSL-VPN appliance in your computers browser. The authentication window is displayed.



Step 2 Enter your username in the **Username** field.

Step 3 The first time you log in to the Virtual office, your entry in the password field depends on whether you have been given a PIN or if you need to create the PIN.

- If you already have a PIN, enter the passcode in the **Password** field. The passcode is the user PIN and the SecurID token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
- If you do not have a PIN, enter the SecurID token code in the **Password** field.

Step 4 Select the appropriate **Domain**.

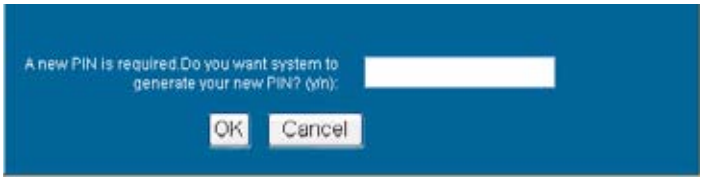
Note If manually entering the Domain, it is case-sensitive.

Step 5 Click **Login**.

Creating a New PIN

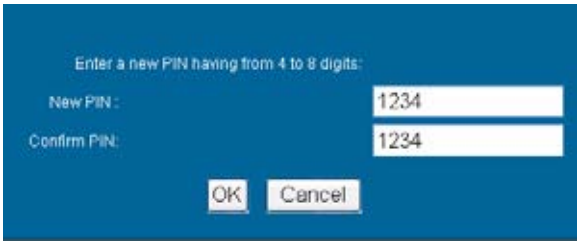
The RSA Authentication Manager automatically determines when users are required to create a new PIN. will determines that user associated with a particular token requires a new PIN. The SSL-VPN appliance prompts the user to enter new PIN.

Step 1 If the user is configured for the **Allowed to Create a PIN** option, users are first asked if they want the system to generate a PIN. To have the system generate a PIN, type **y** and click **OK**. To create your own PIN, type **n** and click **OK**.



Step 2 The new PIN is displayed. To accept the PIN type **y** and click **OK**. To have the system generate a different PIN, type **n** and click **OK**.

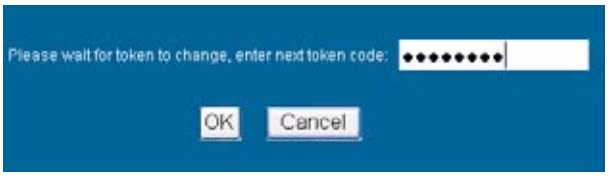
Step 3 If you declined to accept a system-generated PIN, or if your username is configured for **Required to Create a PIN**, you are prompted to enter your new PIN. Enter the PIN in the **New PIN** field and again in the **Confirm PIN** field and click **OK**.



Step 4 The RSA Authentication Manager verifies that the new PIN is an acceptable PIN. If the PIN is accepted, the user is prompted to log in with the new passcode.

Waiting for the Next Token Mode

If user authentication fails three consecutive times, the RSA server requires the user to generate and enter a new token. To complete authentication, the user is prompted to wait for the token to change and enter the next token.



VASCO User Authentication Process

The following sections describe user tasks when using RSA two-factor authentication:

- “Logging into the SSL VPN Virtual Office Using VASCO Two-Factor Authentication” on page 20
- “Creating a New PIN” on page 19

Logging into the SSL VPN Virtual Office Using VASCO Two-Factor Authentication

To log in to the SonicWALL SSL VPN Virtual Office using VASCO two-factor authentication, perform the following steps:

Step 1 Enter the IP address of the SSL-VPN appliance in your computers browser. The authentication window is displayed.

Step 2 Enter your username in the **Username** field.

Step 3 Enter the passcode in the **Password** field. The passcode is the user PIN and the VASCO Digipass token code. For example, if the users PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.

Step 4 Select the appropriate **Domain**.

Note If manually entering the Domain, it is case-sensitive.

Step 5 Click **Login**.

Using One-Time Passwords

The following sections describe how to use one-time passwords:

- User Prerequisites, page 21
- User Configuration Tasks, page 21
- Verifying User One-Time Password Configuration, page 23
- Troubleshooting Common Errors, page 23

User Prerequisites

Users must have a user account enabled in the SSL VPN management interface. Only users enabled by the administrator to use the One-Time Password feature will need to perform the following configuration tasks. The administrator must enable a correct email address that is accessible by the user. Users cannot enable the One-Time Password feature and they must be able to access the SSL VPN Virtual Office portal.

Note The One-Time Password feature is supported on the SonicWALL SSL-VPN 2000, SSL-VPN 4000, and SRA 4200 security appliances.

User Configuration Tasks

To use the One-Time Password feature, perform the following steps:

Step 1 If you are not logged into the SSL VPN Virtual Office user interface, open a Web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** pull-down. Click **Login**.

Step 2 The prompt “A temporary password has been sent to user@email.com” will appear, displaying your pre-configured email account.

Step 3 Login to your email account to retrieve the one-time password.

Step 4 Type or paste the one-time password into the **Password:** field where prompted and click **Login**.

Step 5 You will be logged in to the Virtual Office.

Note One-time passwords are immediately deleted after a successful login, and cannot be used again. Unused one-time passwords will expire according to each user’s timeout policy.

Configuring One-Time Passwords for SMS-Capable Phones

SonicWALL SSL VPN One-Time Passwords can be configured to be sent via email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS.

Below is a list of SMS email formats for selected major carriers, where 4085551212 represents a 10-digit telephone number and area code.

Note These SMS email formats are for reference only. These email formats are subject to change and may vary. You may need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T: 4085551212@mobile.att.net
- Cingular: 4085551212@mobile.mycingular.com
- T-Mobile: 4085551212@tmomail.net
- Nextel: 4085551212@messaging.nextel.com
- Virgin Mobile: 4085551212@vmobl.com
- Qwest: 4085551212@qwestmp.com

For a more complete list, see the *SonicWALL SSL VPN Administrator's Guide*.

Verifying User One-Time Password Configuration

If you are successfully logged in to Virtual Office, you have correctly used the One-Time Password feature.

If you cannot login using the One-Time Password feature, verify the following:

- Are you able to login to the Virtual Office without being prompted to check your email for a one-time password? You have not been enabled to use the One-Time Password feature. Contact your SSL VPN administrator.
- Is your email address correct? If your email address has been entered incorrectly, contact your SSL VPN administrator to correct it.
- Is there no email with a one-time password? Wait a few minutes and refresh your email inbox. Check your spam filter. If there is no email after several minutes, try to login again to generate a new one-time password.
- Have you accurately typed the one-time password in the correct field? Re-type or copy and paste the one-time password.

Troubleshooting Common Errors

Symptom I see an error message indicating that an email configuration is invalid, and I have verified that the One-Time Password feature is configured correctly.

Possible Cause The SonicWALL SSL VPN One-Time Password feature does not support email servers that require passwords or other authentication. Your email server must allow anonymous access to allow the One-Time Password feature to successfully send a one-time password.

Using NetExtender

The following sections describe how to use NetExtender:

- "User Prerequisites" section on page 23
- "User Configuration Tasks" section on page 24
- "Verifying NetExtender Operation from the System Tray" section on page 42

User Prerequisites

Prerequisites for Windows Clients:

Windows clients must meet the following prerequisites in order to use NetExtender:

- One of the following platforms:
  - Windows 7 Beta
  - Windows Vista 64-bit, Windows Vista 32-bit, Windows Vista Service Pack 1
  - Windows XP Home or Professional, Windows XP Service Pack 3
  - Windows 2000 Professional, Windows 2000 Server, Windows 2003 Server.
- One of the following browsers:

  - Internet Explorer 6.0 and higher
  - Mozilla Firefox 1.5 and higher
- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the SSL VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Prerequisites for MacOS Clients:

MacOS clients meet the following prerequisites in order to use NetExtender:

- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

Prerequisites for Linux Clients:

Linux clients must meet the following prerequisites in order to use NetExtender:

- Linux Fedora Core 3 or higher, Ubuntu 7 or higher, or OpenSUSE
- Sun Java 1.4 and higher is required for using the NetExtender GUI.

Note Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.4, you can use the command-line interface version of NetExtender.

User Configuration Tasks

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

The following sections describe how to use NetExtender on the various supported platforms:

Windows Platform Installation

- “Installing NetExtender Using the Mozilla Firefox Browser” section on page 25
- “Installing NetExtender Using the Internet Explorer Browser” section on page 28

Windows Platform Usage

- “Launching NetExtender Directly from Your Computer” section on page 33
- “Configuring NetExtender Preferences” section on page 34
- “Configuring NetExtender Connection Scripts” section on page 36
- “Configuring Proxy Settings” section on page 38
- “Viewing the NetExtender Log” section on page 40
- “Disconnecting NetExtender” section on page 41

- "Upgrading NetExtender" section on page 42
- "Uninstalling NetExtender" section on page 42
- "Verifying NetExtender Operation from the System Tray" section on page 42
- "Using the NetExtender Command Line Interface" section on page 43

MacOS Platform

- "Installing NetExtender on MacOS" section on page 45
- "Using NetExtender on MacOS" section on page 47

Linux Platform

- "Installing and Using NetExtender on Linux" section on page 49

Windows Mobile Platform

- "Installing and Using NetExtender for Windows Mobile" section on page 53

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser, perform the following:

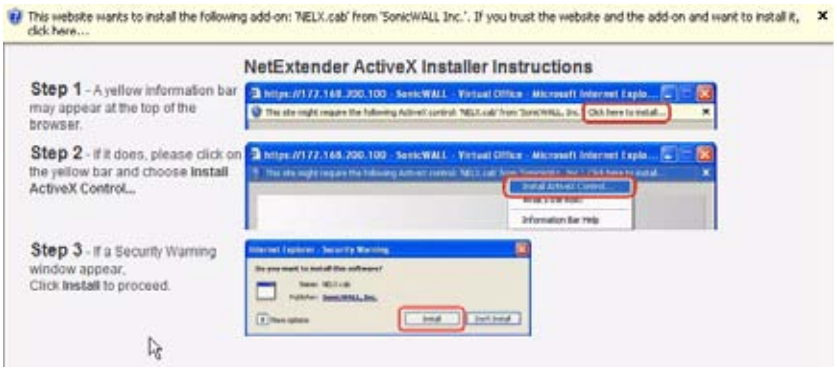
Step 1 To launch NetExtender, first log in to the SSL VPN portal.

Step 2 Click the **NetExtender** button.

Step 3 The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer. If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.

SonicWALL - Virtual Office - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://sslvpn.sonicwall.com/cgi-bin/portal
Firefox prevented this site (sslvpn.sonicwall.com) from asking you to install software on your computer.
Edit Options...
SONICWALL Virtual Office
Options
Help
Logout
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Virtual Assist
Assist someone by taking control of their computer.
Tips/Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.
What is Virtual Assist?

Step 4 The **Allowed Sites - Software Installation** window may appear, with the address of the Virtual Office server in the address window. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.


This website wants to install the following add-on: 'NELX.cab' from 'SonicWALL Inc.'. If you trust the website and the add-on and want to install it, click here...
NetExtender ActiveX Installer Instructions
Step 1 - A yellow information bar may appear at the top of the browser.
Step 2 - If it does, please click on the yellow bar and choose Install ActiveX Control...
Step 3 - If a Security Warning window appear, Click Install to proceed.

Step 5 The **Allowed Sites** window displays. Click **Allow** to add the SSL-VPN appliance to the list of allowed sites.

Allowed Sites - Software Installation
You can specify which web sites are allowed to install software. Type the exact address of the site you want to allow and then click Allow.
Address of web site:
10.0.93.200
Allow
Site
Status
Remove Site
Remove All Sites
Close

Step 6 Return to the **Virtual Office** window and click **NetExtender** again.

Step 7 You may see a security warning. Click **Install**.

Step 8 You may see a Web site certificate warning message. Select the **Accept this certificate permanently** button and click **OK**.

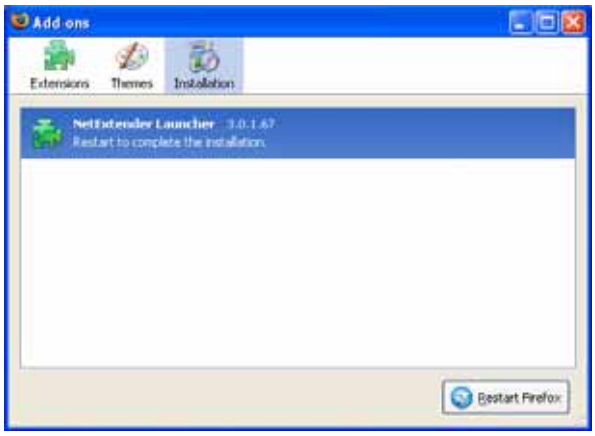
Website Certified by an Unknown Authority
Unable to verify the identity of 192.168.200.1 as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be 192.168.200.1, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site 192.168.200.1?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel

Step 9 You may see a Security Error: Domain Name Mismatch warning. Click **OK**.

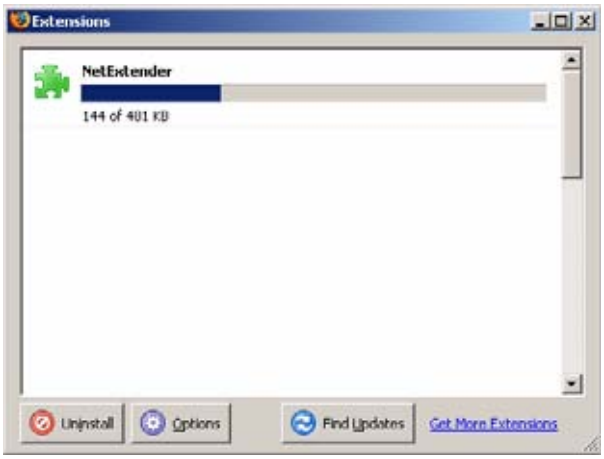
Security Error: Domain Name Mismatch
You have attempted to establish a connection with "10.202.4.40". However, the security certificate presented belongs to "192.168.200.1". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "10.202.4.40", please cancel the connection and notify the site administrator.
View Certificate
OK
Cancel

Step 10 The **Software Installation** window is displayed. After a five second countdown, the **Install Now** button will become active. Click it.

Step 11 You may be prompted to re-start Firefox in order to install NetExtender. Click **Restart FireFox**.



Step 12 Firefox will restart and you will need to login again. NetExtender will then install as a Firefox extension.



Step 13 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.

Closing the windows (clicking on the **x** icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation.

Step 14 Review the following table to understand the fields in the **NetExtender Status** window.

Field	Description
Status	Indicates what operating state the NetExtender client is in, either Connected or Disconnected.
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Duration	The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds.

Step 15 Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.

Step 16 The NetExtender icon is displayed in the task bar.

Installing NetExtender Using the Internet Explorer Browser

SonicWALL SSL VPN NetExtender is fully compatible with Microsoft Windows Vista 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems.

Note It may be necessary to restart your computer when installing NetExtender on Windows Vista.

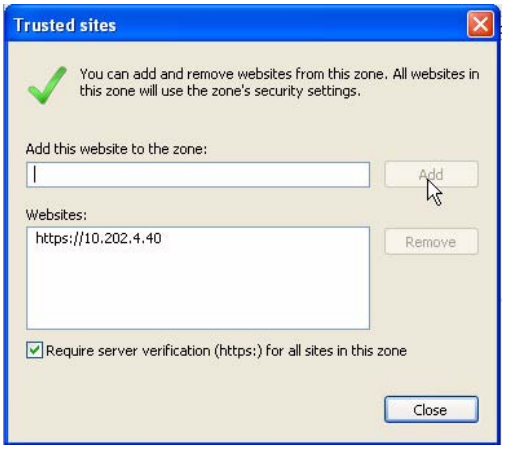
Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SSL VPN server to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Internet Explorer's trusted sites list, complete the following procedure:

Step 1 In Internet Explorer, go to **Tools > Internet Options**.

Step 2 Click on the **Security** tab.

Step 3 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.


Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
https://10.202.4.40
Remove
Require server verification (https:) for all sites in this zone
Close

Step 4 Enter the URL or domain name of your SSL VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 5 Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Internet Explorer browser, perform the following:

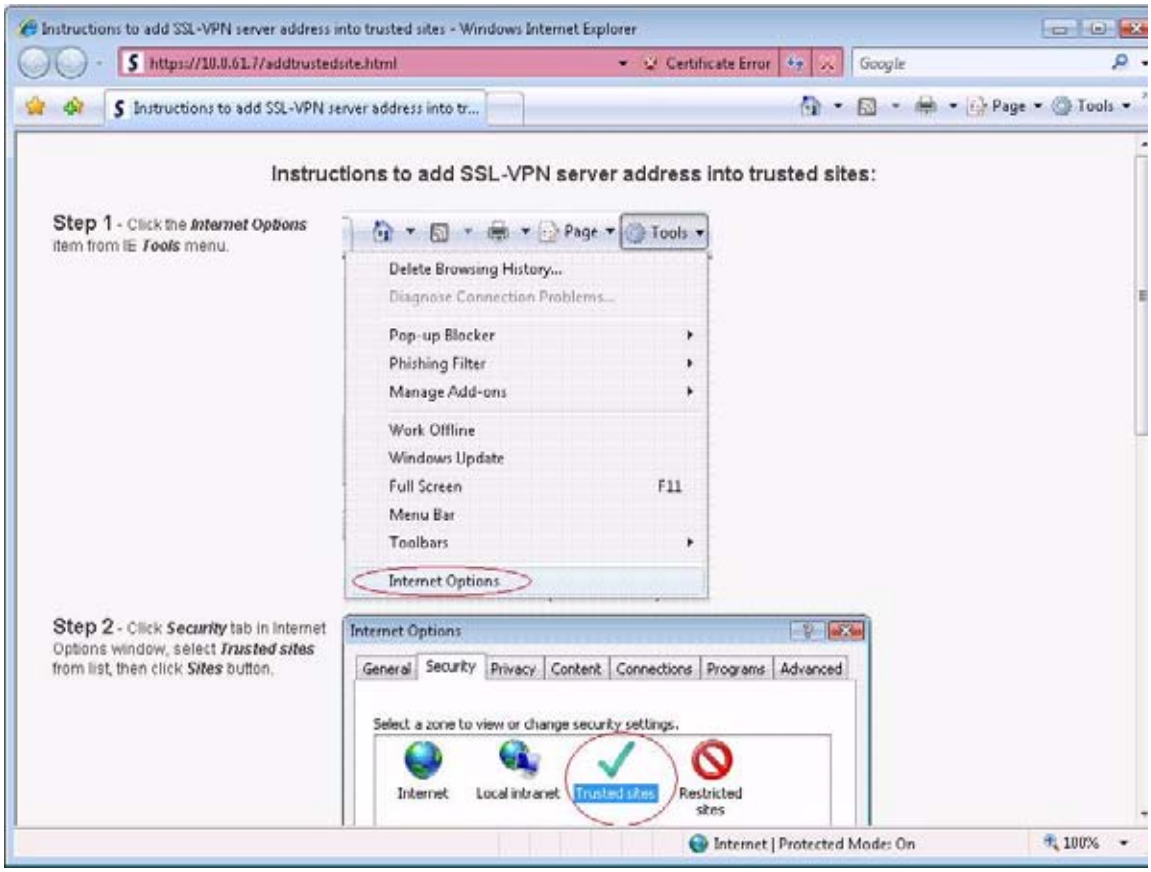
Step 1 Log in to the SSL VPN Virtual Office portal.

Step 2 Click the **NetExtender** button.

Step 3 The first time you launch NetExtender, you must first add the SSL VPN portal to your list of trusted sites. If you have not done so, the follow message will display.

SONICWALL
Welcome, user!
Logout
Help
NetExtender has detected that Microsoft Internet Explorer is running in Protected Mode!
In order to launch NetExtender, you have to add the SSL-VPN server address into trusted sites list.
Instructions to add SSL-VPN server address into trusted sites >>
Copyright © 2007 SonicWALL, Inc.

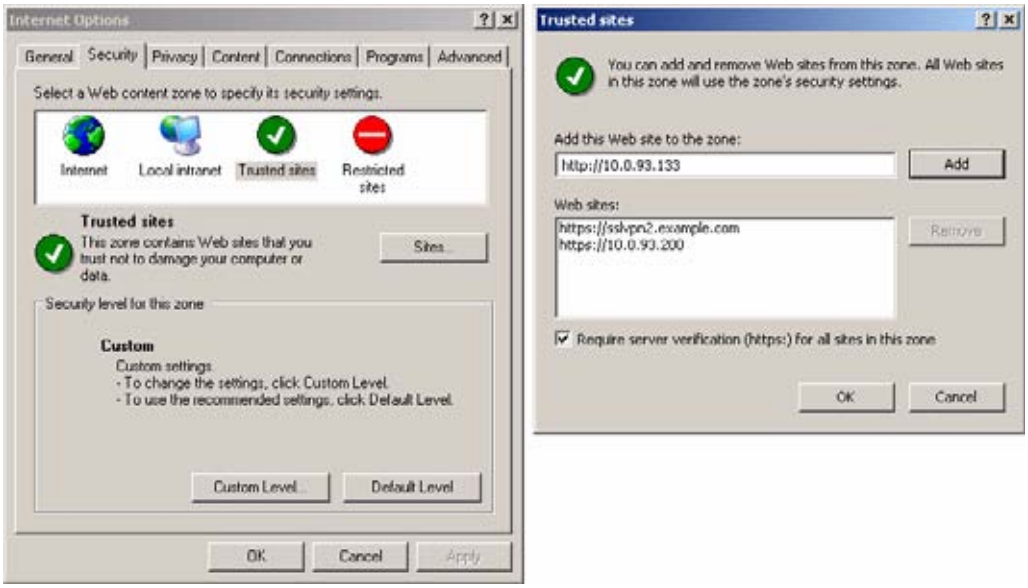
Step 4 Click **Instructions to add SSL VPN server address into trusted sites** for help.



Step 5 In Internet Explorer, go to **Tools > Internet Options**.

Step 6 Click on the **Security** tab.

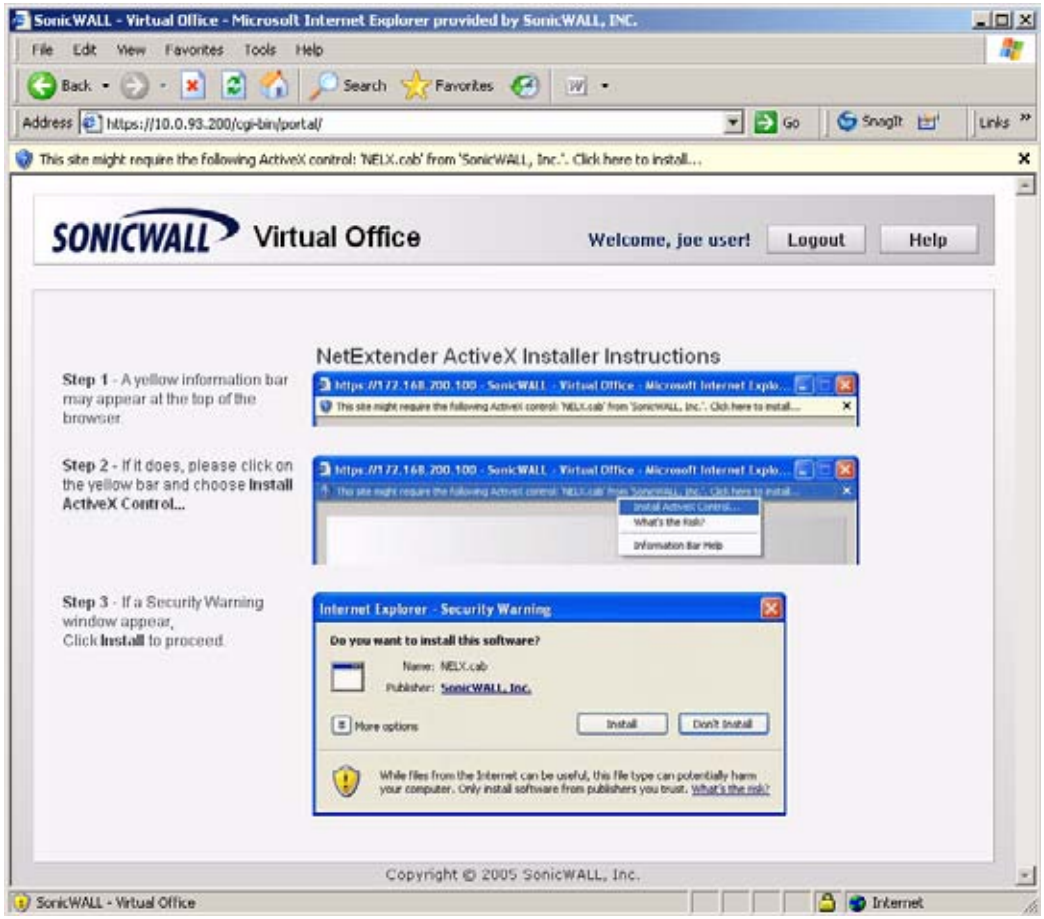
Step 7 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



Step 8 Enter the URL or domain name of your SSL VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 9 Click **OK** in the **Trusted Sites** and **Internet Options** windows.

Step 10 Return to the SSL VPN portal and click on the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.


SonicWALL - Virtual Office - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Address https://10.0.93.200/cgi-bin/portal/
This site might require the following ActiveX control: 'NELX.cab' from 'SonicWALL, Inc.'. Click here to install...
SONICWALL Virtual Office
Welcome, joe user!
Logout
Help
NetExtender ActiveX Installer Instructions
Step 1 - A yellow information bar may appear at the top of the browser.
Step 2 - If it does, please click on the yellow bar and choose Install ActiveX Control...
Step 3 - If a Security Warning window appear, Click Install to proceed.
Internet Explorer - Security Warning
Do you want to install this software?
Name: NELX.cab
Publisher: SonicWALL, Inc.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?
Copyright © 2005 SonicWALL, Inc.
SonicWALL - Virtual Office
Internet

Step 11 If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

Step 12 If a warning message that NetExtender has not passed Windows Logo testing is displayed, click **Continue Anyway**. SonicWALL testing has verified that NetExtender is fully compatible with Windows 7 Beta, Vista, XP, 2000, and 2003.

Hardware Installation
The software you are installing for this hardware:
SSL-VPN NetExtender Adapter
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

Step 13 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.

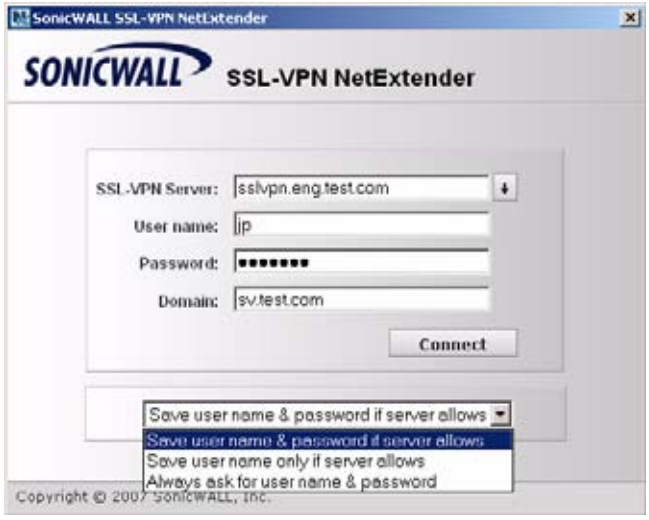
Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal. To launch NetExtender, complete the following procedure:

Step 1 Navigate to **Start > All Programs**.

Step 2 Select the **SonicWALL SSL VPN NetExtender** folder, and then click on **SonicWALL SSL VPN NetExtender**. The NetExtender login window is displayed.

Step 3 The IP address of the last SSL VPN server you connected to is displayed in the **SSL VPN Server** field. To display a list of recent SSL VPN servers you have connected to, click on the arrow.



Step 4 Enter your username and password.

Step 5 The last domain you connected to is displayed in the **Domain** field.

Step 6 The pulldown menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

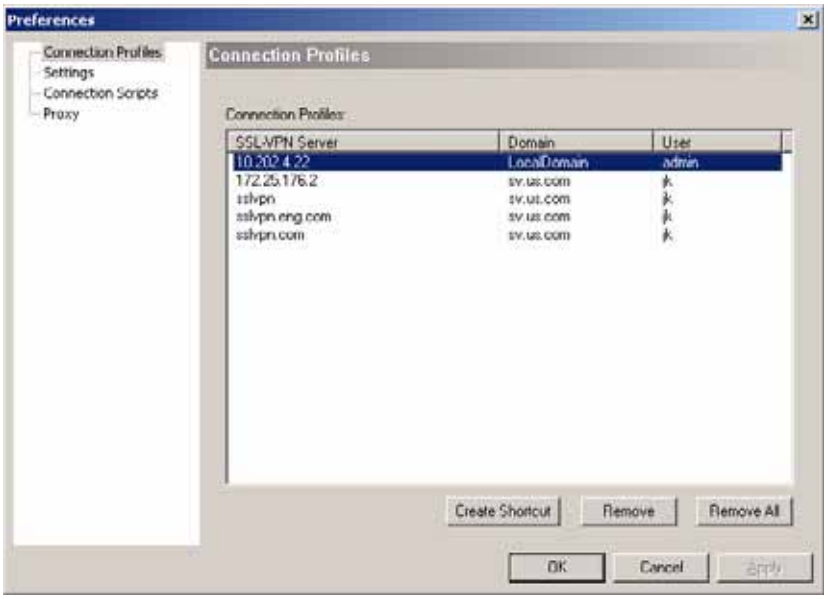
Tip Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

Configuring NetExtender Preferences

Complete the following procedure to configure NetExtender preferences:

Step 1 Right click on the icon in the system tray and click on **Preferences...** The NetExtender Preferences window is displayed.

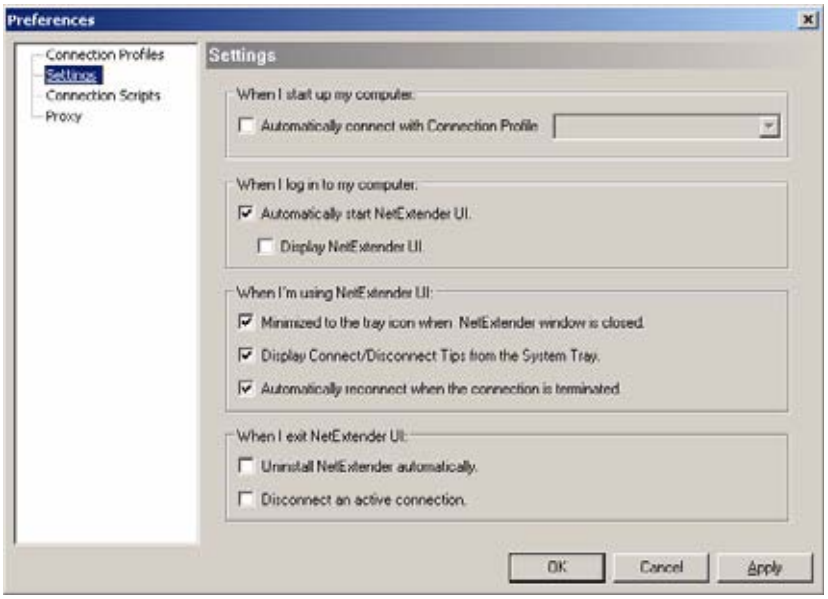
Step 2 The **Connection Profiles** tab displays the SSL VPN connection profiles you have used, including the IP address of the SSL VPN server, the domain, and the username.



Step 3 To create a shortcut on your desktop that will launch NetExtender with the specified profile, highlight the profile and click **Create Shortcut**.

Step 4 To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.

Step 5 The **Settings** tab allows you to customize the behavior of NetExtender.



Step 6 To have NetExtender automatically connect when you start your computer, check the **Automatically connect with Connection Profile** checkbox and select the appropriate connection profile from the pulldown menu.

Note Only connection profiles that allow you to save your username and password can be set to automatically connect.

Step 7 To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray. To have the NetExtender log-in window display, check the **Display NetExtender UI** checkbox.

Step 8 Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window's program menu.

Step 9 Select Display Connect/Disconnect Tips from the System Tray to have NetExtender display tips when you mouse over the NetExtender icon.

Step 10 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

Step 11 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Step 12 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session

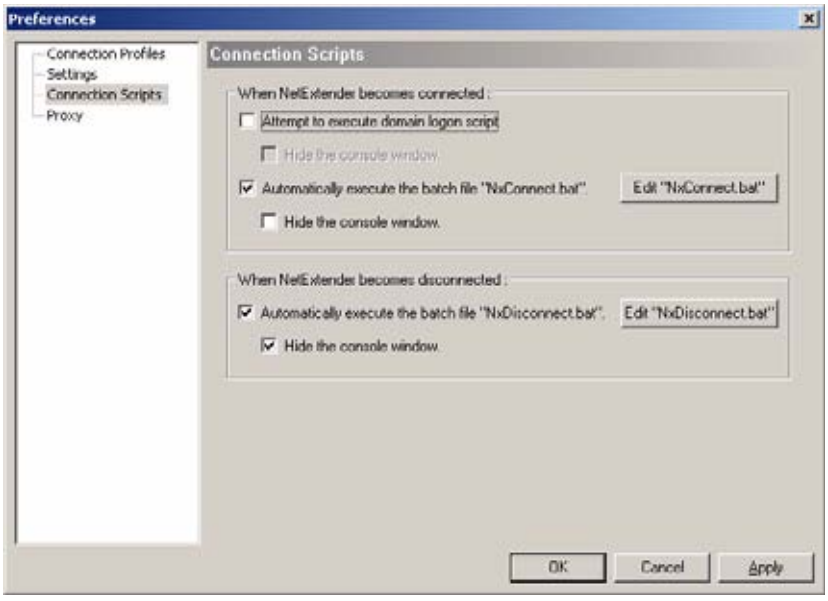
Step 13 Click **Apply**.

Configuring NetExtender Connection Scripts

SonicWALL SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. To configure NetExtender Connection Scripts, perform the following tasks.

Step 1 Right click on the icon in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.

Step 2 Click on **Connection Scripts**.



Step 3 To enable the domain login script, select the **Attempt to execute domain login script** checkbox. When enabled, NetExtender will attempt to contact the domain controller and execute the login script.

Note Enabling this feature may cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible via NetExtender routes.

Step 4 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** checkbox.

Step 5 To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** checkbox.

Step 6 To hide either of the console windows, select the appropriate **Hide the console window** checkbox. If this checkbox is not selected, the DOS console window will remain open while the script runs.

Step 7 Click **Apply**.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

Step 1 To configure the script that runs when NetExtender connects, click the **Edit "NxConnect.bat"** button. The NxConnect.bat file is displayed.

Step 2 To configure the script that runs when NetExtender disconnects, click the **Edit "NxDisconnect.bat"** button. The NxConnect.bat file is displayed.

Step 3 By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. Too add commands, scroll to the bottom of the file.

Step 4 To map a network drive, enter a command in the following format:

net use *drive-letter**server**share password* **/user:***Domain**name*

For example to if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, the command would be the following:

```
net use z\\engineering\docs 1234 /user:eng\admin
```

Step 5 To disconnect a network drive, enter a command in the following format:

net use *drive-letter*: **/delete**

For example, to disconnect network drive z, enter the following command:

```
net use z: /delete
```

Step 6 To map a network printer, enter a command in the following format:

net use LPT1 *ServerName**PrinterNa*me **/user:***Domain**name*

For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is admin, the command would be the following:

```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```

Step 7 To disconnect a network printer, enter a command in the following format:

```
net use LPT1 /delete
```

Step 8 To launch an application enter a command in the following format:

```
C:\Path-to-Application\Application.exe
```

Step 9 For example, to launch Microsoft Outlook, enter the following command:

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

Step 10 To open a Web site in your default browser, enter a command in the following format:

```
start http://www.website.com
```

Step 11 To open a file on your computer, enter a command in the following format:

```
C:\Path-to-file\myFile.doc
```

Step 12 When you have finished editing the scripts, save the file and close it.

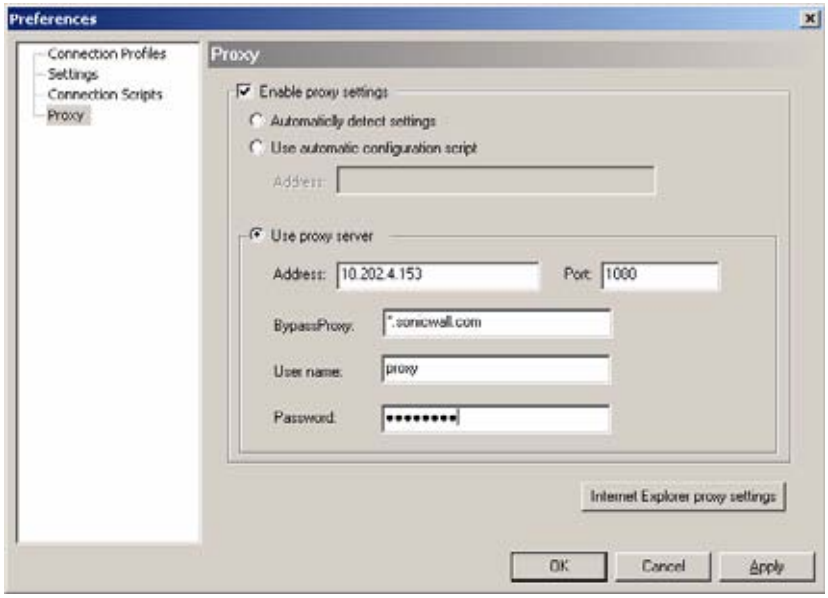
Configuring Proxy Settings

SonicWALL SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings, perform the following tasks.

Step 1 Right click on the icon in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.

Step 2 Click on **Proxy**.



Step 3 Select the **Enable proxy settings** checkbox.

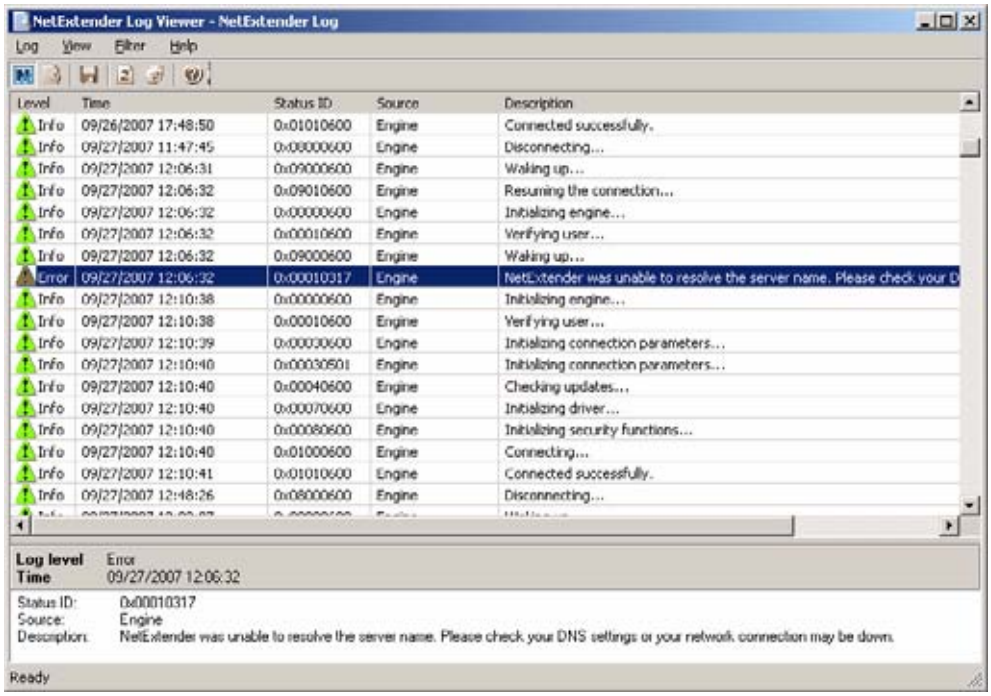
Step 4 NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Preferences** window, a NetExtender pop-up window will prompt you to enter them when you first connect.

Step 5 Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.

Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory: C:\Program Files\SonicWALL\SSL VPN\NetExtender. To view the NetExtender log, right click on the NetExtender icon in the system tray, and click **View Log**.

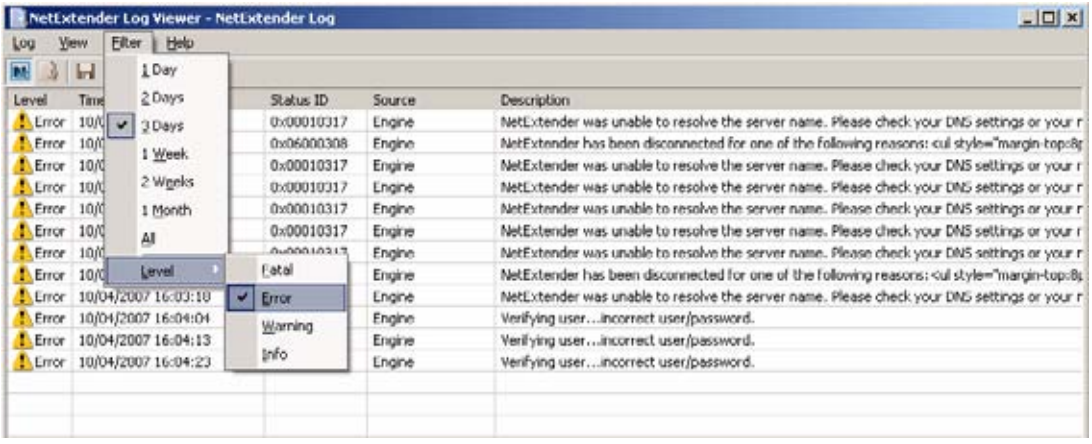

NetExtender Log Viewer - NetExtender Log
Log View Filter Help
Level Time Status ID Source Description
Info 09/26/2007 17:48:50 0x01010600 Engine Connected successfully.
Info 09/27/2007 11:47:45 0x08000600 Engine Disconnecting...
Info 09/27/2007 12:06:31 0x09000600 Engine Waking up...
Info 09/27/2007 12:06:32 0x09010600 Engine Resuming the connection...
Info 09/27/2007 12:06:32 0x00000600 Engine Initializing engine...
Info 09/27/2007 12:06:32 0x00010600 Engine Verifying user...
Info 09/27/2007 12:06:32 0x09000600 Engine Waking up...
Error 09/27/2007 12:06:32 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your D
Info 09/27/2007 12:10:38 0x00000600 Engine Initializing engine...
Info 09/27/2007 12:10:38 0x00010600 Engine Verifying user...
Info 09/27/2007 12:10:39 0x00030600 Engine Initializing connection parameters...
Info 09/27/2007 12:10:40 0x00030501 Engine Initializing connection parameters...
Info 09/27/2007 12:10:40 0x00040600 Engine Checking updates...
Info 09/27/2007 12:10:40 0x00070600 Engine Initializing driver...
Info 09/27/2007 12:10:40 0x00080600 Engine Initializing security functions...
Info 09/27/2007 12:10:40 0x01000600 Engine Connecting...
Info 09/27/2007 12:10:41 0x01010600 Engine Connected successfully.
Info 09/27/2007 12:48:26 0x08000600 Engine Disconnecting...
Log level Error
Time 09/27/2007 12:06:32
Status ID: 0x00010317
Source: Engine
Description: NetExtender was unable to resolve the server name. Please check your DNS settings or your network connection may be down.
Ready

To view details of a log message, double-click on a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export**.

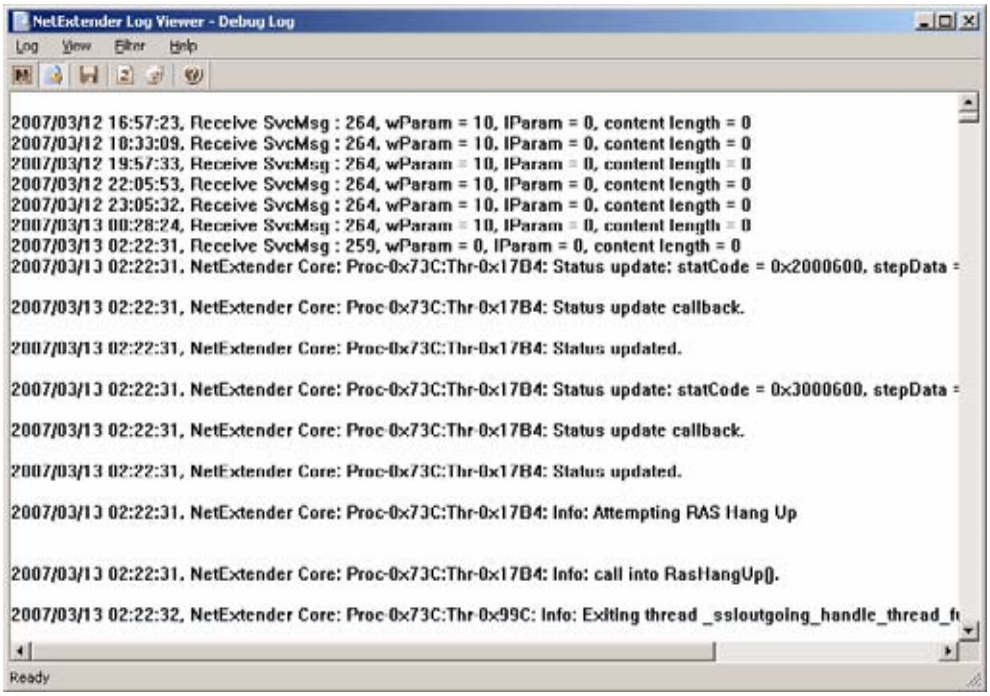
SonicWALL SSL VPN release 2.5 introduces the ability to filter the NetExtender log. To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal**, **Error**, **Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.


NetExtender Log Viewer - NetExtender Log
Log View Filter Help
1 Day
2 Days
3 Days
1 Week
2 Weeks
1 Month
All
Level
Fatal
Error
Warning
Info
Level Status ID Source Description
Error 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error 0x06000308 Engine NetExtender has been disconnected for one of the following reasons:
Error 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error 0x00010317 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error Engine NetExtender has been disconnected for one of the following reasons:
Error 10/04/2007 16:03:10 Engine NetExtender was unable to resolve the server name. Please check your DNS settings or your r
Error 10/04/2007 16:04:04 Engine Verifying user...incorrect user/password.
Error 10/04/2007 16:04:13 Engine Verifying user...incorrect user/password.
Error 10/04/2007 16:04:23 Engine Verifying user...incorrect user/password.

To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.

Note It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.


NetExtender Log Viewer - Debug Log
Log View Filter Help
2007/03/12 16:57:23, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/12 18:33:09, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/12 19:57:33, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/12 22:05:53, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/12 23:05:32, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/13 00:28:24, Receive SvcMsg : 264, wParam = 10, lParam = 0, content length = 0
2007/03/13 02:22:31, Receive SvcMsg : 259, wParam = 0, lParam = 0, content length = 0
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status update: statCode = 0x2000600, stepData =
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status update callback.
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status updated.
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status update: statCode = 0x3000600, stepData =
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status update callback.
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Status updated.
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Info: Attempting RAS Hang Up
2007/03/13 02:22:31, NetExtender Core: Proc-0x73C:Thr-0x17B4: Info: call into RasHangUp().
2007/03/13 02:22:32, NetExtender Core: Proc-0x73C:Thr-0x99C: Info: Exiting thread _ssloutgoing_handle_thread_f
Ready

To clear the log, click on **Log > Clear Log**.

Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

Step 1 Right click on the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.

Step 2 Wait several seconds. The NetExtender session disconnects.

You can also disconnect by double clicking on the NetExtender icon to open the **NetExtender** window and then clicking the **Disconnect** button.

When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

Upgrading NetExtender

Beginning with SonicWALL SSL VPN release 2.5, NetExtender automatically notifies users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the SonicWALL SSL-VPN security appliance.

SonicWALL SSL-VPN NetExtender
SONICWALL
SSL-VPN NetExtender
A new version of NetExtender is required to connect to the SSL-VPN server, click OK to upgrade
OK
Copyright © 2007 SonicWALL, Inc.

When using releases prior 2.5, users should periodically launch NetExtender from the SonicWALL Virtual Office to ensure they have the latest version. Prior to release 2.5, the standalone NetExtender does not check for updates when it is launched directly from a user's computer.

Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **SonicWALL SSL VPN NetExtender**, and then click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected. To do so, perform the following steps:

Step 1 Right click on the NetExtender icon in the system tray and click on **Preferences**... The **NetExtender Preferences** window is displayed.

Step 2 Click on the **Settings** tab.

Step 3 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the NetExtender icon in the system tray. The following are some tasks you can perform with the system tray.

Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.

Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray.

Using the NetExtender Command Line Interface

SonicWALL SSL VPN release 3.5 introduces a command line interface (CLI) for controlling NetExtender.

Note The NetExtender command line interface is only available on Windows platforms.

To launch the NetExtender CLI, perform the following tasks:

Step 1 Launch the Windows Command Prompt by going to the **Start** menu, select **Run**, enter **cmd**, and click **OK**.

Step 2 Change directory to where NetExtender is installed. To do this, you first must enter **cd ../..** to move up to the root drive. The enter **cd Program Files\SonicWALL\SSL-VPN\NetExtender**.

Step 3 Enter **NECLI.exe**. The NetExtender CLI launches and displays a summary of the available commands.

```
C:\Program Files\SonicWALL\SSL-VPN\NetExtender>NECLI.exe

                          ,,,,,,,,,,,,,,,
          ,,,mmbbbbbb1111111111111111111111bbbbbmm,,,
   ,,,b||PPPPPPP||```````````````|PPPPPPPPP111111111111bbm,,
 ``````                                    `````PPPP111111111bm,
                                                ```PP1111111bm,
                                                    `PP111111b,
                                                       |111111:
NECLI for Windows - Version 3. 5. 0. 1                  .1111P|.
Copyright (C) 2008 SonicWALL Inc.                      ,b1PP|`
                                                     ,,||```
```

Table 1 describes the commands available in the NetExtender CLI and their options.

Table 1 NetExtender CLI Commands

Command	Options	Description
NECLI connect		Initiates a NetExtender session.
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
NECLI createprofile		Creates a NetExtender profile
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
NECLI deleteprofile		Deletes a saved NetExtender profile.
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-d *domain-name*	The domain to connect to.
NECLI disconnect		Disconnects
NECLI displayprofile		Displays all NetExtender profiles.
	-s *server*	(Optional) Displays only the profiles that are saved for the specified server.
	-u *user-name*	(Optional) Displays only the profiles that are saved for the specified user name.
	-d *domain-name*	(Optional) Displays only the profiles that are saved for the specified domain name.
NECLI queryproxy		Checks the connect to the proxy server.
NECLI reconnect		Attempts to reconnect to the server.

Table 1 NetExtender CLI Commands

NECLI showstatus		Displays the status of the current NetExtender session.
NECLI setproxy		Configures proxy settings for NetExtender.
	-t [**1** | **2** | **3**]	There are three options for setting proxy settings: • **1** - Automatically detects proxy settings. The proxy server must support Web Proxy Auto Discovery Protocol (WPAD). • **2** - Uses a proxy script. • **3** - Manually configure the proxy server.
	-s proxy address	The address of the proxy script or proxy server.
	-o port	The port number.
	-u user name	The user name for the proxy server.
	-p password	The password name for the proxy server.
	-b bypass-proxy	Bypasses the previously configured proxy settings.
	-save	Saves the proxy settings.
NECLI viewlog		Displays the NetExtender log.

Installing NetExtender on MacOS

SonicWALL SSL VPN supports NetExtender on MacOS. To use NetExtender on your MacOS system, your system must meet the following prerequisites:

- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

To install NetExtender on your MacOS system, perform the following tasks:

Step 1 Log in to the SonicWALL Virtual Office.

Step 2 Click the **NetExtender** button.

Step 3 The Virtual Office displays the status of NetExtender installation. A pop-up window may appear, prompting you to accept a certificate. Click **Trust**.

SONICWALL Virtual Office
Welcome, jp!
Logout
Help
NetExtender for Mac OS X
In the future, you can launch NetExtender from your Applications folder without returning to this web page.
Return to Virtual Office
Copyright © 2008 SonicWALL, Inc.
sslvpn.eng.sonicwall.com
Do you want to accept this certificate from the web site "sslv.com" for the purpose of exchanging encrypted information?
Publisher authenticity can not be verified.
Show Certificate
Don't Trust
Trust

Step 4 A second pop-up window may appear, prompting you to accept a certificate. Click **Trust**.

https://sslvpn.eng.sonicwall.com
This applet was signed by "SonicWALL, Inc.," and authenticated by "Thawte Consulting cc". Do you trust this certificate?
Click Trust to run this applet and allow it unrestricted access to your computer. Click Don't Trust to run this applet with standard Java restrictions.
Show Certificate
Don't Trust
Trust

Step 5 When NetExtender is successfully installed and connected, the NetExtender status window displays.

Using NetExtender on MacOS

Step 1 To launch NetExtender, go the **Applications** folder in the **Finder** and double click on **NetExtender.app**.

Step 2 The first time you connect, you must enter the SonicWALL SSL VPN server name in the **SSL VPN Server** field.

Step 3 Enter your username and password.

Step 4 The first time you connect, you must enter the **domain** name.

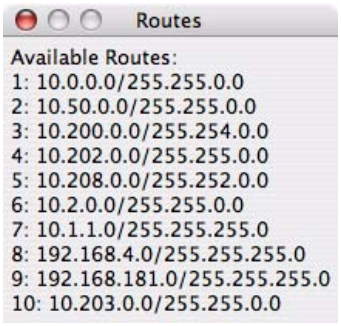
Step 5 Click **Connect**.

Step 6 You can instruct NetExtender remember your profile server name in the future. In the **Save profile** pulldown menu you can select **Save name and password (if allowed)**, **Save username only (if allowed)**, or **Do not save profile**.

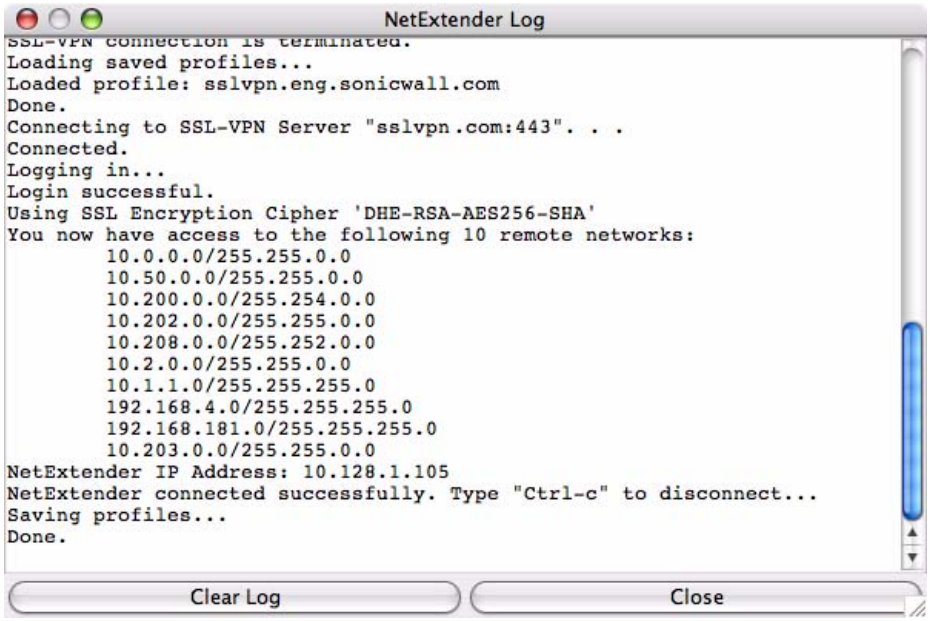
Step 7 When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

Step 8 To display a summary of your NetExtender session, click **Connection Status.**

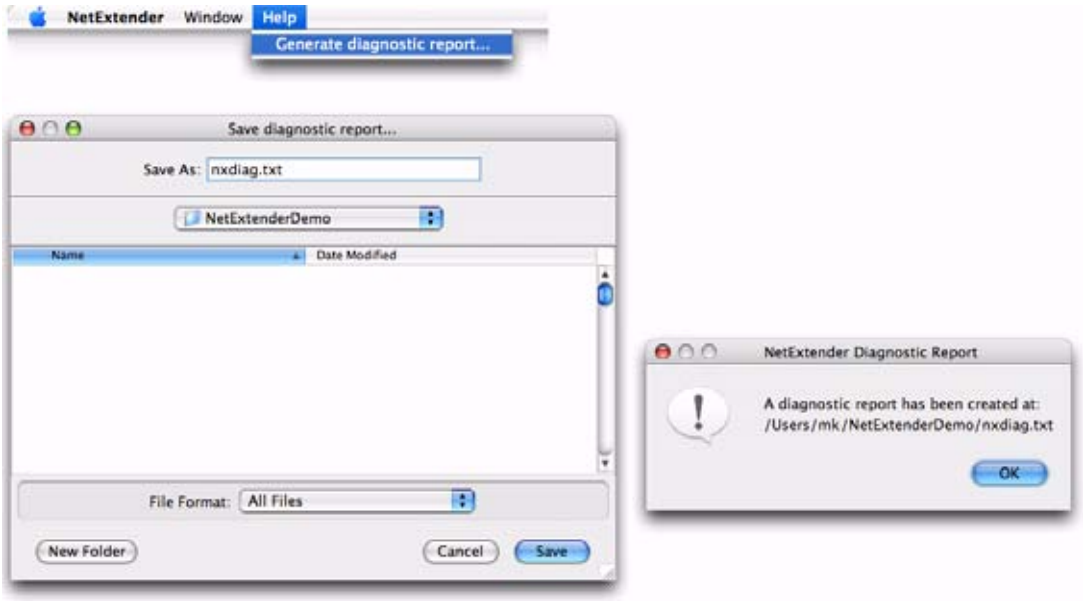
Step 9 To view the routes that NetExtender has installed, go to the **NetExtender** menu and select **Routes**.



Step 10 To view the NetExtender Log, go to **Window > Log**.



Step 11 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



Step 12 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Installing and Using NetExtender on Linux

SonicWALL SSL VPN supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

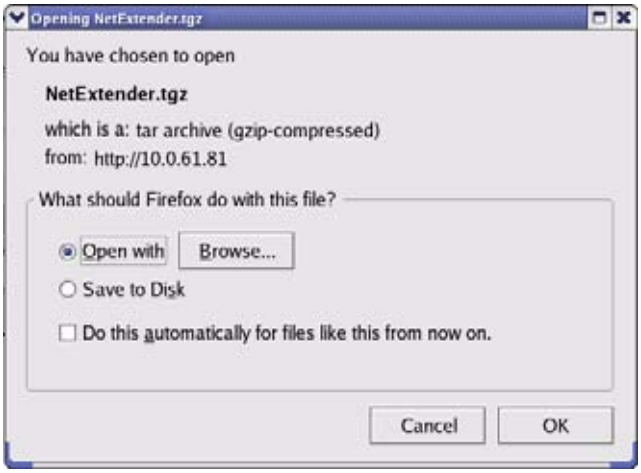
- i386-compatible distribution of Linux
- Linux Fedora Core 3+, Ubuntu 7+ or OpenSUSE Linux 10.3+
- Sun Java 1.4 and higher is required for using the NetExtender GUI.

Note Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.4, you can use the command-line interface version of NetExtender.

To install NetExtender on your Linux system, perform the following tasks:

Step 1 Log in to the SonicWALL Virtual Office.

Step 2 Click the **NetExtender** button. A pop-up window indicates that you have chosen to open the **NetExtender.tgz** file. Click **OK** to save it to your default download directory.



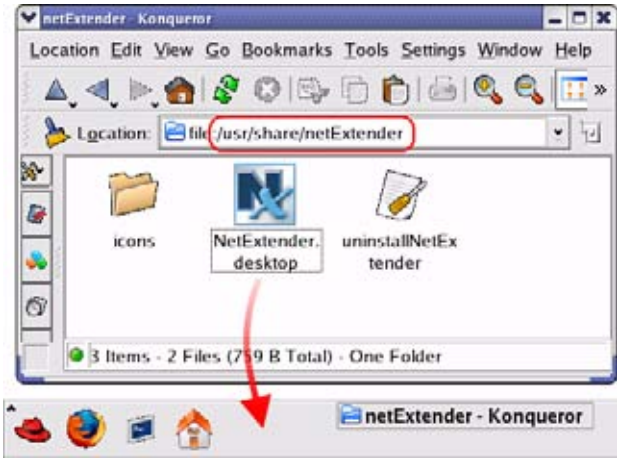
Step 3 To install NetExtender from the CLI, navigate to the directory where you saved **NetExtender.tgz** and enter the **tar -zxf NetExtender.tgz** command.

mk:~/netExtenderClient - Shell - Konsole
[mk~]$ tar -zxf NetExtender.tgz
[mk~]$ cd netExtenderClient
[mk netExtenderClient]$ ./install
--- SonicWALL NetExtender 2.5.17 Installer ---
Please run the NetExtender installer as root.
On many systems, you can use the sudo command:
[mk netExtenderClient]$ sudo ./install
Password:
--- SonicWALL NetExtender 2.5.17 Installer ---
Checking library dependencies...
Checking pppd...
Copying files...
---------- INSTALLATION SUCCESSFUL ----------
Type 'netExtenderGui' to launch NetExtender.
Look in /usr/share/netExtender for a desktop shortcut and icon files.
[mk netExtenderClient]$

Step 4 Type the **cd netExtenderClient** command.

Step 5 Type **./install** to install NetExtender.

Step 6 Launch the **NetExtender.tgz** file and follow the instructions in the NetExtender installer. The new netExtender directory contains a NetExtender shortcut that can be dragged to your desktop or toolbar.



Step 7 The first time you connect, you must enter the SonicWALL SSL VPN server name in the **SSL VPN Server** field. NetExtender will remember the server name in the future.

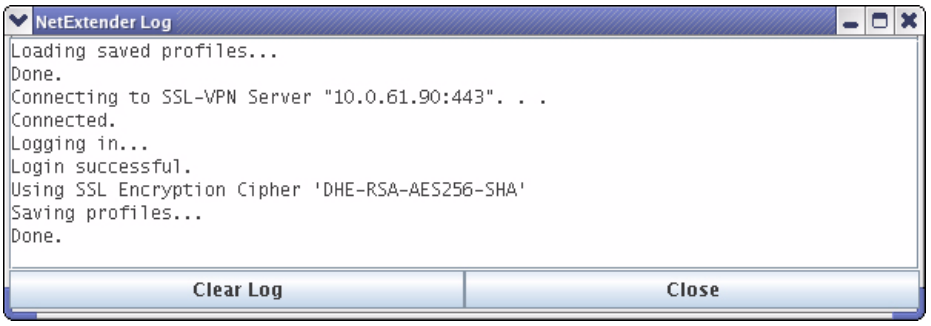
Step 8 Enter your username and password.

Step 9 The first time you connect, you must enter the **domain** name. NetExtender will remember the domain name in the future.

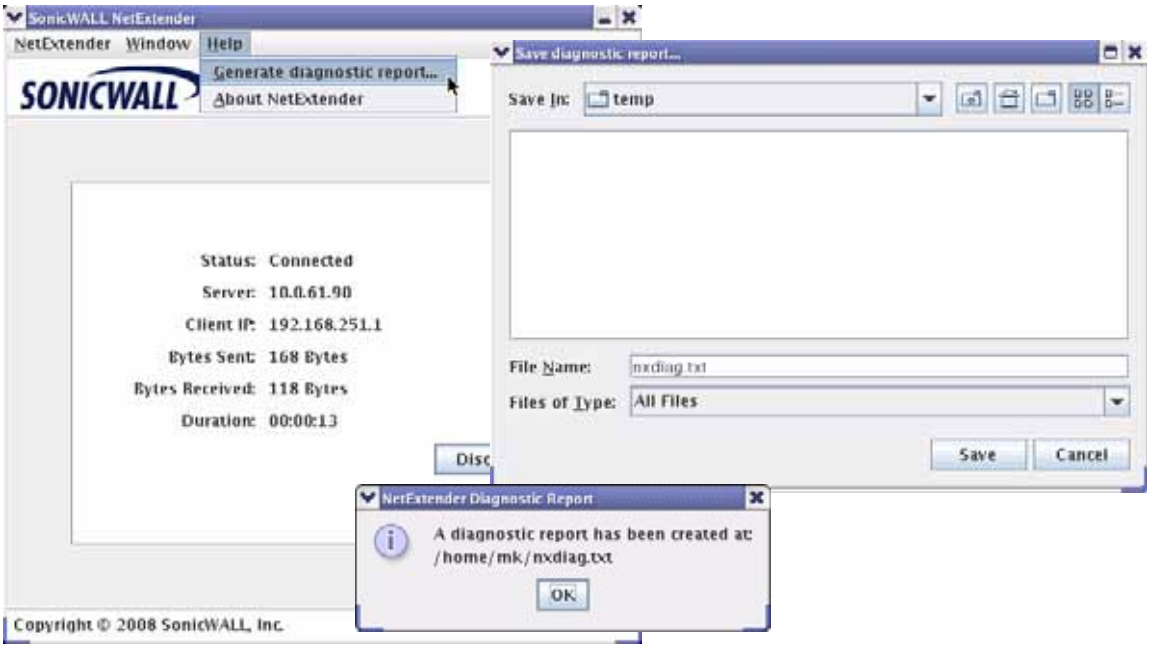
Note You must be logged in as root to install NetExtender, although many Linux systems will allow the **sudo ./install** command to be used if you are not logged in as root.

Step 10 To view the NetExtender routes, go to the **NetExtender** menu and select **Routes**.

Step 11 To view the NetExtender Log, go to **NetExtender > Log**.



Step 12 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



Step 13 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Installing and Using NetExtender for Windows Mobile

SonicWALL SSL VPN now supports NetExtender for the Windows Mobile platform. NetExtender for Windows Mobile provides the following features:

- One-time passwords
- Two-factor authentication
- HTTP proxy
- Connection profiles

NetExtender supports the following Windows Mobile platforms:

- Windows Mobile 5 PocketPC version
- Windows Mobile 6 Professional/Classic version

Note Windows Mobile 5 Smart Phone version and Windows Mobile 6 Standard version are not currently supported.

To use NetExtender on your Windows Mobile device, perform the following tasks:

Step 1 Navigate to the URL or IP address for your SSL VPN Virtual Office using the browser in your Windows Mobile device.

Step 2 Log in with your username and password.

Step 3 Click on the **NetExtender** icon.

Step 4 Follow the on-screen instructions to install NetExtender. When NetExtender is installed, you may be prompted to restart your device. Click **Yes**.

Step 5 From your Windows Mobile device, launch NetExtender. The NetExtender login screen displays.

Step 6 Enter the IP address or domain name for your SSL VPN server in the **Server** field. The IP address of the last SSL VPN server you connected to is displayed by default. To display a list of recent SSL VPN servers you have connected to, click on the arrow.

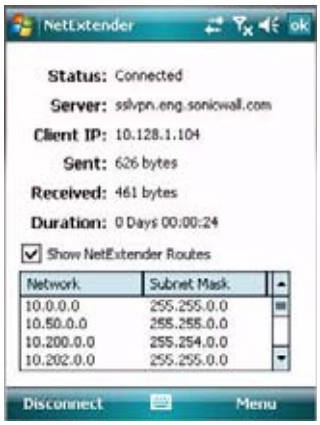
Step 7 Enter your username and password.

Step 8 The last domain you connected to is displayed in the **Domain** field.

Step 9 The pulldown menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

Step 10 Click **Connect**. When NetExtender successfully connects, the NetExtender Status window displays.



Step 11 To configure NetExtender options, click the **Menu** button. The following options are displayed:

- **Connection Profiles** - Displays all of the NetExtender connections that you have used on this device. To remove a Connection Profile, highlight the profile, click the **Menu** button, and click **Remove**.

- **System Settings** - Provides several configuration options.

  - **Hide NetExtender when closing window** - Hides NetExtender when you click the **ok** button.
  - **Display precise number in status** - Displays the exact numbers of sent and receive data.
  - **Use Connection Manager to establish underlying connections** - Uses the Windows Mobile Connection Manager to establish the device's connection to the mobile network. The Connection Manager is designed to determine the optimum network type (such as 3G or wi-fi). If this option is disabled, the user manages the connection manually.
  - **Enable NetExtender log** - Records log entries for NetExtender events.
  - **Overwrite the previous log when NetExtender starts** - Maintains a single NetExtender log file that is overwritten with each new NetExtender session. Disabling this option will create a separate log file for each NetExtender session.

- **Proxy Settings** - Provides the ability to manually specify a proxy server.

Related Documents

The following Technical Notes provide more information on advanced NetExtender scenarios:

- Running NetExtender on a Different TCP Port
- Using the SonicWALL CDP Agent over a SonicWALL NetExtender Connection
- Using SonicWALL NetExtender to Access FTP Servers
- Resolving NetExtender Error With McAfee Enterprise 8.5

Using Virtual Assist

Virtual Assist is an easy to use tool that allows SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Virtual Assist is a lightweight, thin client that installs automatically using Java from the SonicWALL SSL VPN Virtual Office without requiring the installation of any external software. For computers that do not support Java, Virtual Assist can be manually installed by downloading an executable file from the Virtual Office.

Before using Virtual Assist, you must meet the following requirements:

- Virtual Assist is only supported on deployments utilizing the SSL-VPN 2000, SSL-VPN 4000, and SRA 4200 platforms.
- Virtual Assist is only supported on Windows platforms. Virtual Assist is certified to work on Windows Vista, Windows XP and Windows 2000.

There are two sides to a Virtual Assist session: the customer view and the technician view. The customer is the person requesting assistance on their computer. The technician is the person providing assistance. A Virtual Assist session consists of the following sequence of events:

1. The technician launches Virtual Assist from the SonicWALL SSL VPN Virtual Office.
2. The technician monitors the Assistance Queue for customers requesting assistance.
3. The customer requests assistance by one of these methods:
   - Logs into the SonicWALL SSL VPN Virtual Office and clicks on the Virtual Assist link.
   - Receives an email invitation from the technician and clicks on the link to launch Virtual Assist.

- Navigate directly to the URL of the Virtual Assist home page that is provided by the technician.

4. The Virtual Assist application installs and runs on the customer's system.
5. The customer appears in the Virtual Assist Assistance Queue.
6. The technician clicks on the customers name and launches a Virtual Assist session.
7. The technician's Virtual Assist window now displays the customers entire display. The technician has complete control of the customer computer's mouse and keyboard. The customer sees all of the actions that the technician performs.
8. If at anytime the customer wants to end the session, they can take control and click on an **End Virtual Assist** button in the bottom right corner of the screen.
9. When the session ends, the customer resumes sole control of the computer.

The following sections describe how to use Virtual Assist:

- "Launching a Virtual Assist Technician Session" section on page 57
- "Performing Virtual Assist Technician Tasks" section on page 61
- "Using Virtual Assist from the Customer View" section on page 65

Launching a Virtual Assist Technician Session

To launch a Virtual Assist session as a technician, perform the following steps.

Step 1 Log in to the SonicWALL SSL-VPN security appliance Virtual Office. If you are already logged in to the SonicWALL SSL VPN customer interface, click on the **Virtual Office** button.

Step 2 Click on the **Virtual Assist** button.

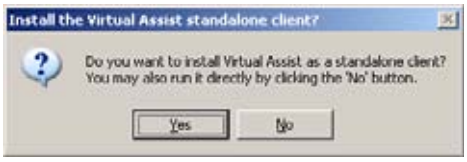
Step 3 The File Download window displays, and Virtual Assist attempts to automatically install. Click **Run** to launch the program directly, or click **Save** to save the installer file to your computer, and then manually launch it.

File Download - Security Warning
Do you want to run or save this file?
Name: ...40-443-085WOi1eb5z13Gjrt70A1g==-admin-0.exe
Type: Application
From: 10.202.4.40
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

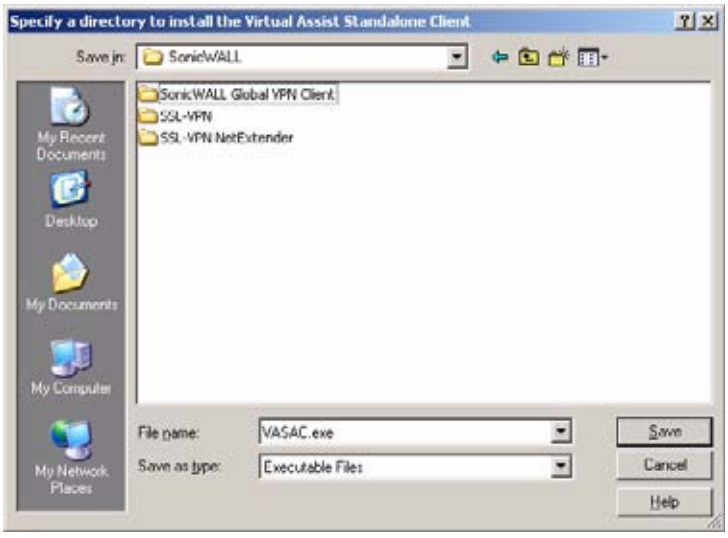
Step 4 When you launch the installer, you may see an additional warning message. Click **Run**.

Internet Explorer - Security Warning
Do you want to run this software?
Name: VASAC-10.202.4.40-443-0ISWOi1eb5z13GjYt70A3g==.exe
Publisher: SonicWALL Inc.
More options
Run
Don't Run
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Step 5 A pop-up window asks if you would like to install Virtual Assist as a standalone client. Click **Yes** to save the application. A shortcut will be added to your desktop and a link to the application will be added to the program list on your Start Menu. Click **No** to launch Virtual Assist without saving the application for future use.


Install the Virtual Assist standalone client?
Do you want to install Virtual Assist as a standalone client? You may also run it directly by clicking the 'No' button.
Yes
No

Step 6 If you clicked **Yes** to save the application, you will be prompted to select a location to save the file. Select an appropriate location, such as C:\Program Files\SonicWALL.



Step 7 When Virtual Assist launches for the first time, you may see a security warning pop-up window. De-select the **Always ask before opening this file** checkbox to avoid this window in the future. Click **Run**.

Open File - Security Warning
Do you want to run this file?
Name: VASAC.exe
Publisher: SonicWALL Inc.
Type: Application
From: C:\Program Files\SonicWALL
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

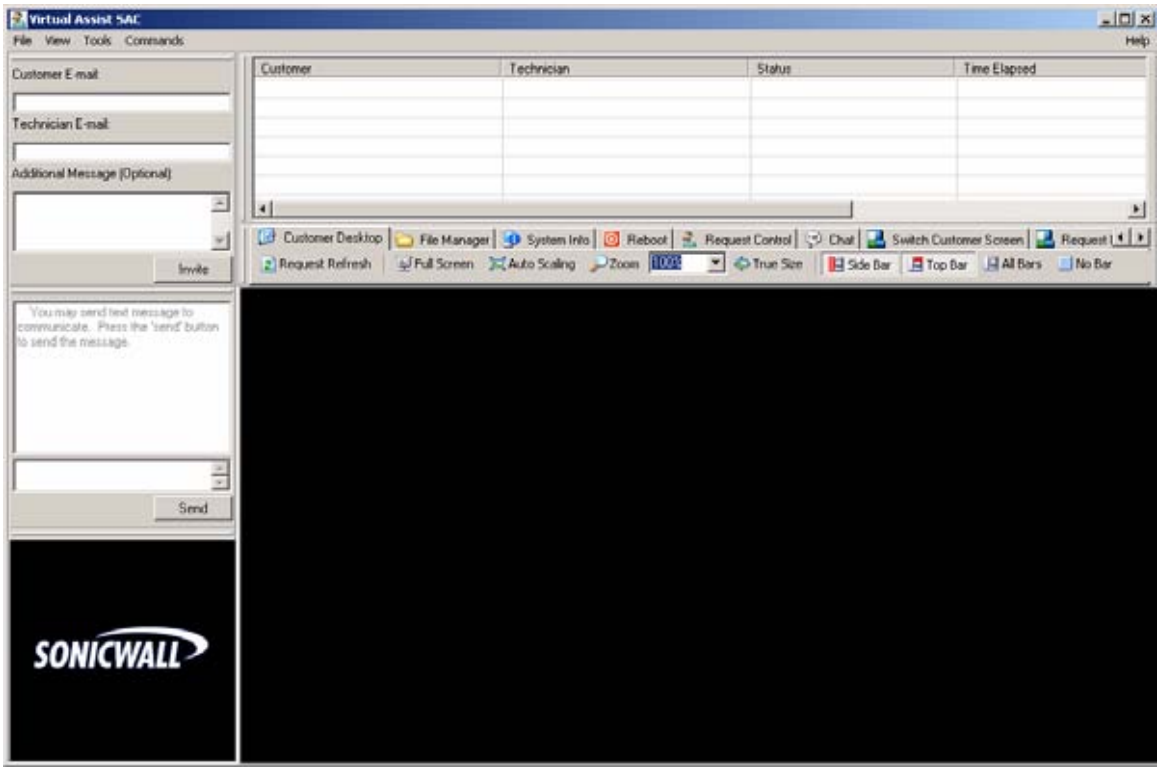
Step 8 The Virtual Assist login window displays.

Step 9 Enter the following information and click **Login**:

- **Server** - The IP address or domain name of SonicWALL SSL-VPN appliance.
- **Username** and **Password** - The username and password for the technician's account on the appliance.
- **Domain** - The domain name for the portal. The default value is LocalDomain.

Note The domain name is case sensitive.

Step 10 The Virtual Assist standalone application launches.



Step 11 The technician is now ready to assist customers.

Performing Virtual Assist Technician Tasks

To get started, the technician logs into the SonicWALL SSL-VPN appliance and launches the Virtual Assist application.

Note Each technician can only assist one customer at a time.

Once the technician has launched the Virtual Assist application, the technician can assist customers by performing the following tasks:

- "Inviting Customers by Email" on page 61
- "Assisting Customers" on page 62
- "Using the Virtual Assist Taskbar" on page 63
- "Using the Virtual Assist File Transfer" on page 64
- "Controlling the Virtual Assist Display" on page 65

Inviting Customers by Email

Step 1 To invite a customer to Virtual Assist, use the email invitation form on the left of the Virtual Assist window.

Note Customers who launch Virtual Assist from an email invitation can only be assisted by the technician who sent the invitation. Customers who manually launch Virtual Assist can be assisted by any technician.

Step 2 Enter the customer's email address in the **Customer E-mail** field.

Step 3 Optionally, enter **Technician E-mail** to use a different return email address than the default technician email. Some mail servers require that an email address be entered, and that it be on a valid domain.

Step 4 Optionally, enter an **Additional Message** to the customer.

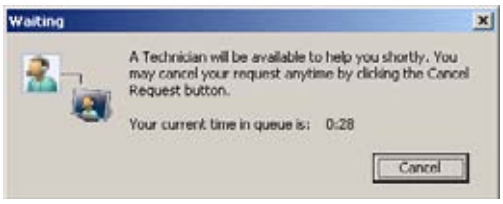
Step 5 Click **Invite**. The customer will receive an email with an HTML link to launch Virtual Assist.

Step 6 Customers requesting assistance will appear in the Assistance Queue, and the duration of time they have been waiting will be displayed.

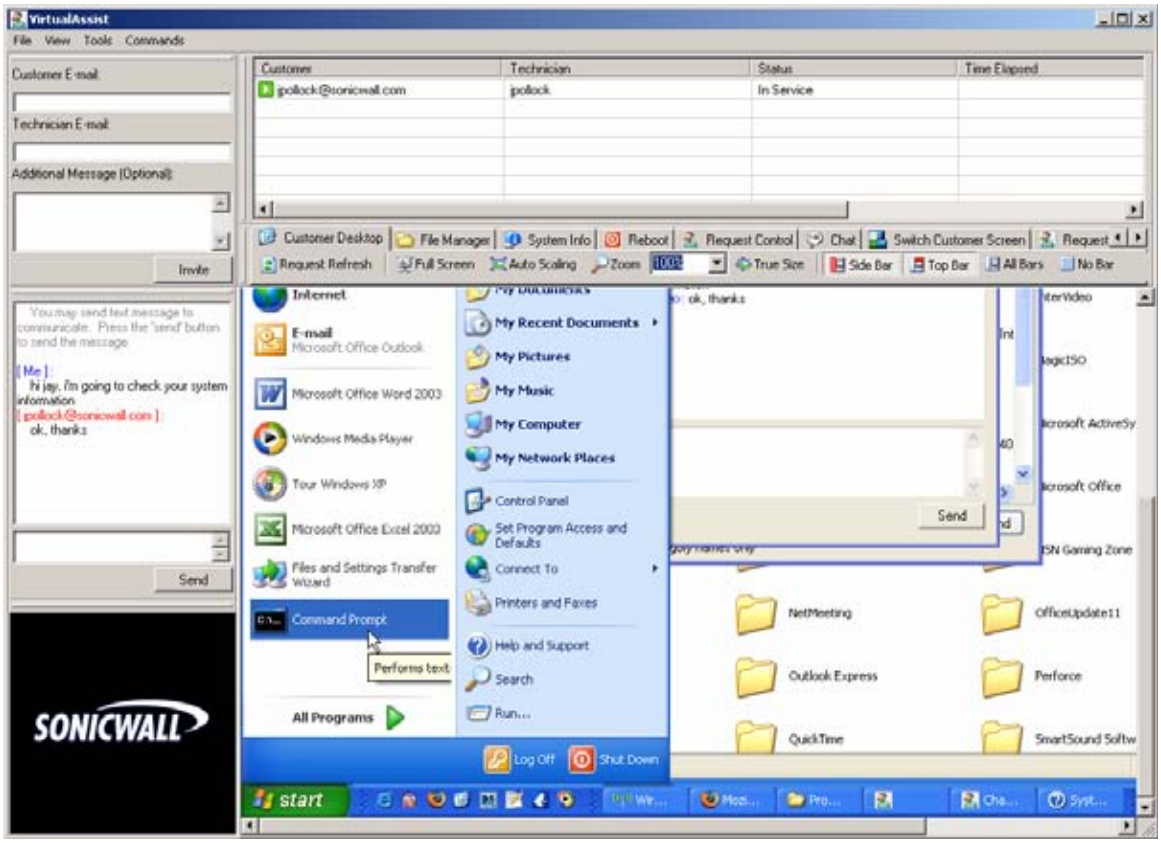
Assisting Customers

Step 1 A pop-up window alerts the technician when a customer is in the assistance queue.

Step 2 Double-click on a customer's user name to begin assisting the customer.


Waiting
A Technician will be available to help you shortly. You may cancel your request anytime by clicking the Cancel Request button.
Your current time in queue is: 0:28
Cancel

Step 3 The customer's entire desktop is displayed in the bottom right window of the Virtual Assist application.



The technician now has complete control of the customer's keyboard and mouse. The customer can see all of the actions that the technician performs.

During a Virtual Assist session, the customer is not locked out of their computer. Both the technician and customer can control the computer, although this may cause confusion and consternation if they both attempt "to drive" at the same time.

The customer has a small tool bar in the bottom right of their screen, with three options.

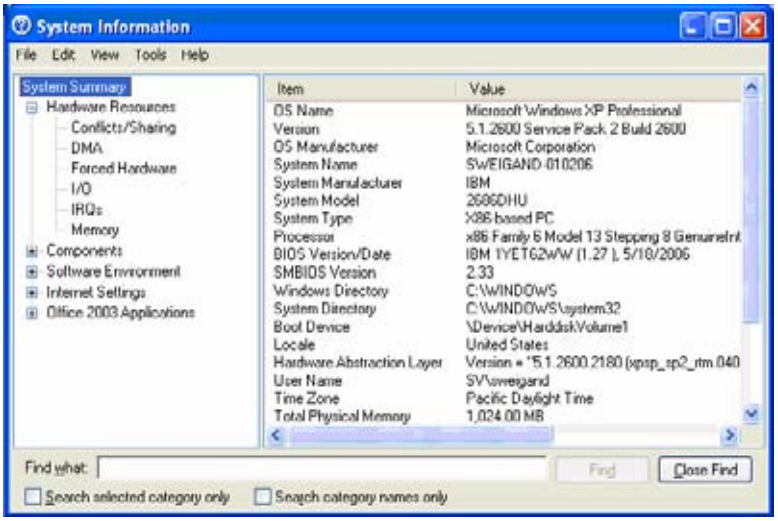
The customer has the following options during a Virtual Assist session:

- **Active** - Toggles to the **View Only** mode, where the technician can view the customer's computer but cannot control the computer.
- **Chat** - Initiates a chat window with the technician.
- **End Virtual Assist** - Terminates the session.

Using the Virtual Assist Taskbar

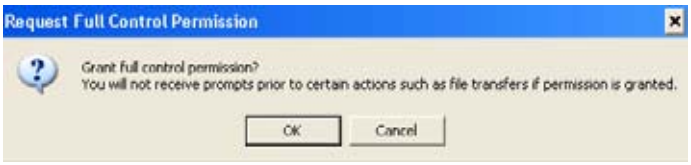
The Technician's view of Virtual Assist includes a taskbar with a number of options.

- **File Transfer** - Launches a window to transfer files to and from the customer's computer. See the "Using the Virtual Assist File Transfer" section on page 64 for more information.
- **System Info** -Displays detailed information about the customer's computer.



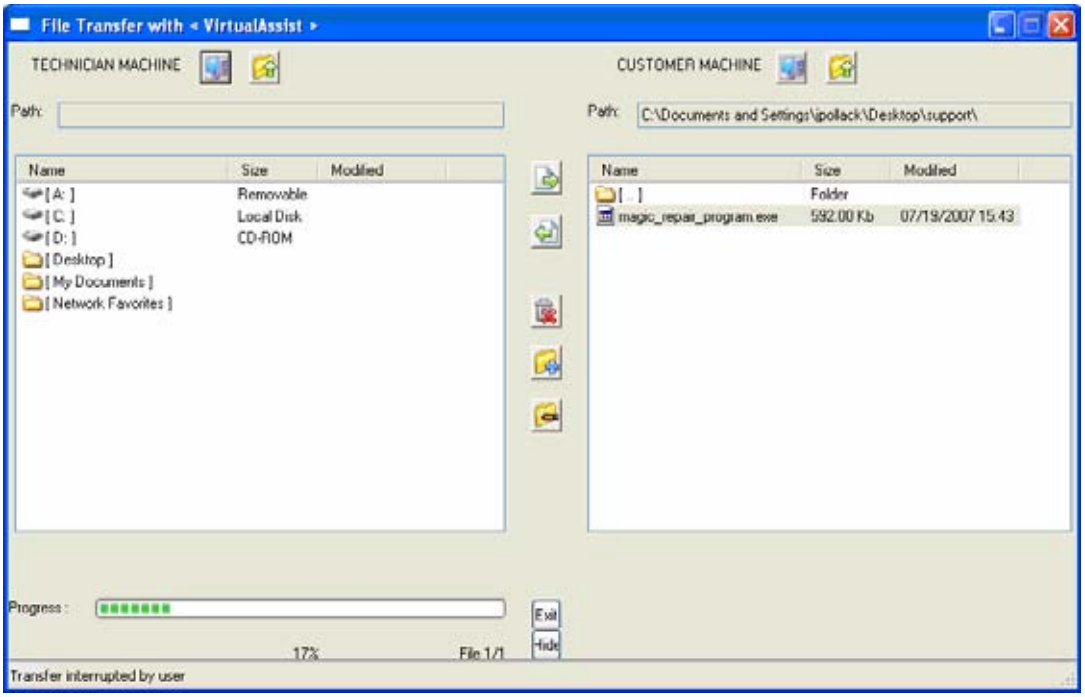
- **Reboot** - Reboot the customer's computer. Unless you have Requested full control, the customer will be warned about and given the opportunity to deny the reboot.
- **Request Control** - If the customer has switched to view-only mode, click the button to prompt the customer to give you control of their system again.
- **Chat** - Launches the chat window to communicate with the customer. The technician can also use the dedicated chat window in the bottom left window of the Virtual Assist application.
- **Switch Customer Screen** - Switches to a second monitor if the customer's computer has more than one monitor configured.

- **Request Full Control -** Allows the technician to reboot the system, delete files, or over-write files on the customer's computer without the customer being prompted for permission first.


Request Full Control Permission
Grant full control permission?
You will not receive prompts prior to certain actions such as file transfers if permission is granted.
OK
Cancel

Using the Virtual Assist File Transfer

The File Transfer window is used to transfer files to and from the customer's computer. The file directory of the technician's computer is shown on the left and the customer's computer on the right.



The File Transfer window functions in much the same manner as Windows Explorer or an FTP program. Navigate the File Transfer window by double-clicking on folders and selecting files. The File Transfer window includes the following controls:

- **Desktop** jumps to the desktop of the technician's or customer's computer.
- **Up** navigates up one directory on either the technician's or customer's computer.
- **Download** transfers the selected file or files from the technician's computer to the customer's computer.
- **Upload** transfers the selected file or files from the customer's computer to the technician's computer.
- **Delete** deletes the selected file or files.

Note When deleting or over-writing files, the customer is warned and must give the technician permission unless the technician has clicked the **Request Full Control** button and the customer has confirmed.

- **New folder** creates a new folder in the selected directory.
- **Rename** renames the selected file or directory.

When a file is transferring, the transfer progress is displayed at the bottom of the File Transfer window. Click the **Exit** button to cancel a transfer in progress.

Note File Transfer supports the transfer of single or multiple files. It does not currently support the transfer of directories. To select multiple files, hold down the **Ctrl** button while clicking on the files.

Controlling the Virtual Assist Display

- **Request Refresh** - Refreshes the display of the customer's computer.
- **Full Screen** - Hides all of the Virtual Assist toolbars and displays the customer's desktop on the technician's entire screen with the Virtual Assist taskbar in the top left corner.

If the Virtual Assist taskbar doesn't display, move your mouse to the top middle of the screen. Right-click on the taskbar and click **Restore** to exit full-screen mode.

- **Auto Scaling** - Zooms the display to fill the entire Virtual Assist window.
- Zoom - Zooms the display to one of several presets or allows you enter a specific value.
- **True Size** - Zooms to 100%.
- **Side Bar** - Toggles the display of the side bar with the email invitation and chat windows.
- **Top Bar** - Toggles the display of the top bar with the customer queue and toolbar.
- **All Bars** - Displays both the side bar and top bar.
- **No Bars** - Hides both the side bar and top bar.

Note A number of these options can be configured from the pull-down menus at the top of the Virtual Assist application.

Using Virtual Assist from the Customer View

Note SSL VPN release 3.5 introduces Virtual Assist customer support for Mac systems. The Mac verison of Virtual Assist supports only the basic connect and control features (and not advanced features such as chat and file transfer).

To launch a Virtual Assist customer session to request help on your computer, perform the following steps:

Step 1 There are several methods for accessing Virtual Assist:

- Navigate to the URL of the Virtual Assist home page that is provided by your support technician.
- If you received an email invitation, click on the link in the email or paste the URL into your Web browser.
- The login page of your Virtual Office may include a direct link to Virtual Assist as shown below.

- Or you may need to login to the Virtual Office and click the **Virtual Assist** button.

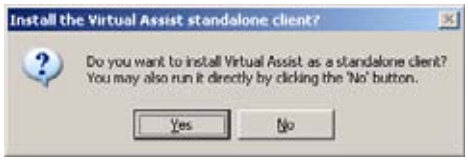
Step 2 The File Download window displays, and Virtual Assist attempts to automatically install. Click **Run** to launch the program directly, or click **Save** to save the installer file to your computer, and then manually launch it.

File Download - Security Warning
Do you want to run or save this file?
Name: ...40-443-0SSWOiLeb5z13GJrt70A3g==-admin-0.exe
Type: Application
From: 10.202.4.40
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

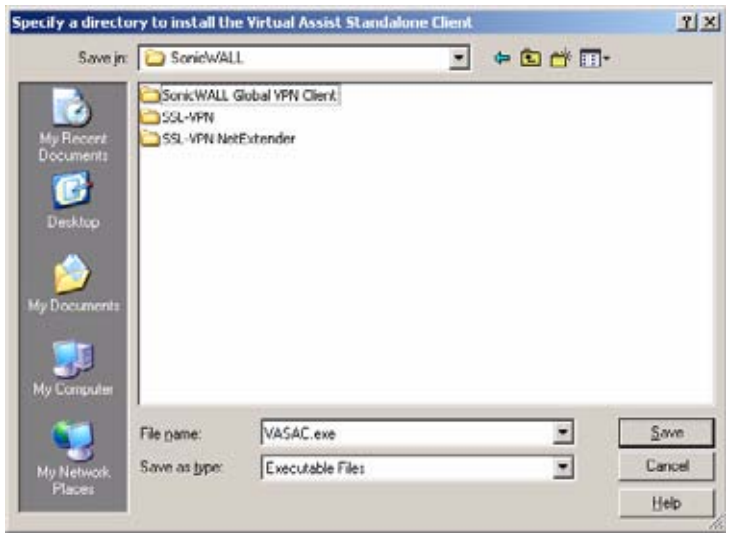
Step 3 When you launch the installer, you may see an additional warning message. Click **Run**.

Internet Explorer - Security Warning
Do you want to run this software?
Name: VASAC-10.202.4.40-443-0ISWOi1eb5z13GJyt70A3g==.exe
Publisher: SonicWALL Inc.
More options
Run
Don't Run
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Step 4 A pop-up window asks if you would like to install Virtual Assist as a standalone client. Click **Yes** to save the application. A shortcut will be added to your desktop and a link to the application will be added to the program list on your Start Menu. Click **No** to launch Virtual Assist without saving the application for future use.


Install the Virtual Assist standalone client?
Do you want to install Virtual Assist as a standalone client? You may also run it directly by clicking the 'No' button.
Yes
No

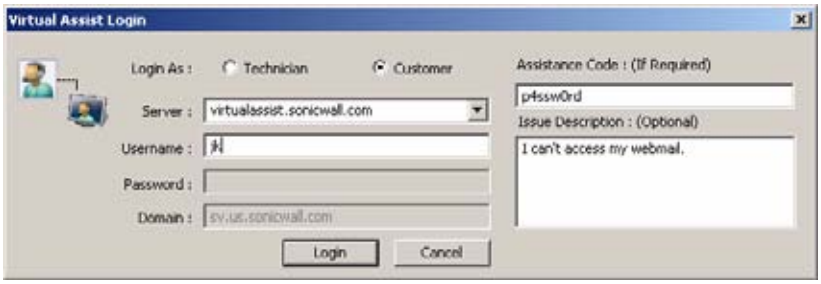
Step 5 If you clicked **Yes** to save the application, you will be prompted to select a location to save the file. Select an appropriate location, such as C:\Program Files\SonicWALL.



Step 6 When Virtual Assist launches for the first time, you may see a security warning pop-up window. De-select the **Always ask before opening this file** checkbox to avoid this window in the future. Click **Run**.

Open File - Security Warning
Do you want to run this file?
Name: VASAC.exe
Publisher: SonicWALL Inc.
Type: Application
From: C:\Program Files\SonicWALL
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Step 7 If you launched Virtual Assist from an email invitation, the application launches directly to the customer queue. If you manually launched the Virtual Assist application or launched it from the Virtual Office, the login window displays.



Step 8 Enter the following information and click **Login**:

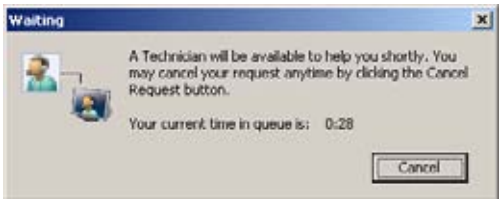
- **Login As** - Select **customer**.
- **Server** - The IP address, IPv6 address, or hostname of the SonicWALL SSL-VPN appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).
- **Username** - Enter your name.
- **Assistance Code** - If the technician provided you with an assistance code, enter it here.
- **Issue Description** - Optionally, you can enter a brief description of your problem.

Step 9 Click **Login**.The Virtual Assist standalone application launches.

Step 10 If you receive the following security alert, click **Unblock** to allow Virtual Assist traffic through the Windows firewall.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: SWTunnel
Publisher: Unknown
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Step 11 A pop-up window indicates that you are in the Virtual Assist queue. The technician will be alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.


Waiting
A Technician will be available to help you shortly. You may cancel your request anytime by clicking the Cancel Request button.
Your current time in queue is: 0:28
Cancel

Step 12 When the technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The technician now has control of your computer.

Note During a Virtual Assist session, you are not completely locked out of your computer. Both the technician and customer can control the computer, although this may cause confusion and consternation if they both attempt to “drive” at the same time. You can resume control when the technician is not actively typing or moving the mouse. And you can end the session at any time by clicking the **End Virtual Assist** button in the bottom right corner.

Step 13 Click the **Chat** button or enter **Alt-c** to open an instant message style chat session with the technician. The Chat button is located in the bottom right corner of your desktop next to the **End Virtual Assist** button.

Step 14 The technician can also open a Chat window to communicate with you. To chat, type text in the **Chat** window and type **Enter** or click **Send**.

Chat with Technician
You may send text message to communicate. Press the 'send' button to send the message.
<Me>: hey there, can you see this?
<Technician>: yep, the connection is good
Send

Step 15 To regain sole control of your computer while still allowing the technician to view your system, click the **Active** button in the bottom right corner.

Step 16 The **Active** button changes to display **View Only**, indicating that you are in View Only mode. Click **View Only** to give the technician control again.

Step 17 You can end the Virtual Assist session at anytime by clicking on the **End Virtual Assist** button in the bottom right corner of the screen, or by entering **Alt-q**. This will end the technician's control of your computer.

Using File Shares

File shares provide remote users with a secure Java applet or HTML-based interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

The File Shares Applet mimics Windows Explorer navigation and provides functionality not available in HTML-based File Shares, including the ability to overwrite existing files and upload directories.

This section contains the following subsections:

- "Using the File Shares Applet" section on page 71
- "Using HTML-Based File Shares" section on page 84

Using the File Shares Applet

The File Shares Applet has a similar look and feel to the Windows Explorer tool, featuring drag-and-drop and multiple file selection capabilities. It also provides the user the ability to set up bookmarks to quickly navigate through networks from the portal level. This feature saves time lost moving through network and server paths. The File Shares Applet leverages Sun's Java platform browser plug-in to increase usability by mimicking the common Windows Explorer interface. With the help of the HTTPS protocol, the applet securely transfers encrypted files and information to and from the SSL-VPN appliance. The appliance communicates this data to the individual machines on the remote network.

This section contains the following subsections:

- "User Prerequisites" section on page 71
- "Configuration Overview" section on page 71
- "Configuration Examples" section on page 76

User Prerequisites

The SonicWALL SSL VPN File Shares Applet is a Java application that supports Java 1.3.1 and newer, and the JRE Version 5.0 Update 10 or newer is recommended. To download the latest Java and JRE versions, visit http://www.java.com. Internet Explorer 6.0, Firefox 1.5 or newer, Opera 8 or newer, and Safari RSS are recommended Web browsers of optimal performance of the Java File Shares feature.

The administrator must enable the File Shares Applet for users to use it.

There must be a computer with open access for the SonicWALL SSL VPN File Shares Applet to log into. The remote computer must have shared folders for files to be copied or moved. Sharing policy must be set from within the remote computer's own operating system.

Configuration Overview

The SSL VPN File Shares Applet is easy and intuitive to use. User should be aware of its functions and limitations. Setting up bookmarks and the browser interface are covered in this section, along with an overview of the browser and sample use cases.

This section contains the following subsections:

- "Setting up Bookmarks" section on page 71
- "Using the Java File Shares Applet" section on page 73
- "File Shares Applet Browser Overview" section on page 75

Setting up Bookmarks

Bookmarks can be set up for folders and for files. A file bookmark will not launch the Applet, but instead will download and launch the file directly. Bookmarks must be enabled by the administrator.

To set up bookmarks from the Virtual Office Portal, perform the following steps.

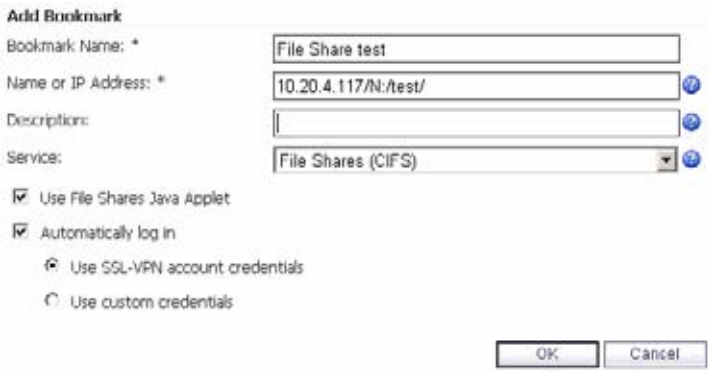
Step 1 Open a Web browser and log into the SSL VPN Virtual Office interface by typing the URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** pull-down. Click **Login**.

Step 2 Click the **Show Edit Controls** link in the middle of the portal page.

Step 3 Click the **New Bookmark** tab in the portal page.

Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Virtual Assist
Assist someone by taking control of their computer.
All Bookmarks
Web
Files
Hide Edit Controls
New Bookmark
Create a new bookmark
FTP Eagle
File Transfer Protocol
User Bookmark
Web (HTTP)
Import Certificate
Tips/Help
Search Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.
What is Virtual Assist?
Virtual Assist allows you to remotely support customers by taking control of their computers while the customer observes.
How can I add more bookmarks?
Click "Show Edit Controls" (above the bookmark table, toward the right-hand side), then click "New Bookmark". If either of these options are missing, your administrator may not have given you permission to add bookmarks.

Step 4 The Add Bookmark screen displays. Enter a friendly name for the bookmark in the **Bookmark Name** field.



Step 5 Enter the IP address and file directory path to the File Share in the **Name or IP Address** field.

Note When using the Java applet, the **Name or IP Address** field must be to a file directory and end with a / or \ character.

Step 6 In the **Service** pull down menu, select the **File Shares (CIFS)** option.

Step 7 Check the **Use File Shares Java Applet** box to enable the File Shares Applet for this bookmark. Leaving this box unchecked means the portal will launch the original HTML browser when the bookmark is selected.

Step 8 Optionally, select **Automatically log in** to log in to this file share using either your SSL VPN credentials or by specifying custom credentials.

Step 9 Click **Add**.

Bookmark serve as useful shortcuts to quickly access different network locations. Bookmarks can also be set up from the File Shares Browser, either by clicking the **Bookmark** button, or using the bookmark option from the right-click menu.

Using the Java File Shares Applet

While loading the browser interface, warning messages might display. These messages will look different for different browsers. For the purpose of these examples, Internet Explorer 6.0 was used.

Step 1 If you are not logged into the SSL VPN Virtual Office user interface, open a Web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** pull-down. Click **Login**.

Step 2 Launch File Shares Applet by clicking the **File Shares** button, or clicking on a link with the File Shares Applet enabled. The File Shares Applet will launch in a new window, separate from the Virtual Office portal.

Step 3 Depending on available browser and Java plug-in, a warning may display, click **OK** to continue.

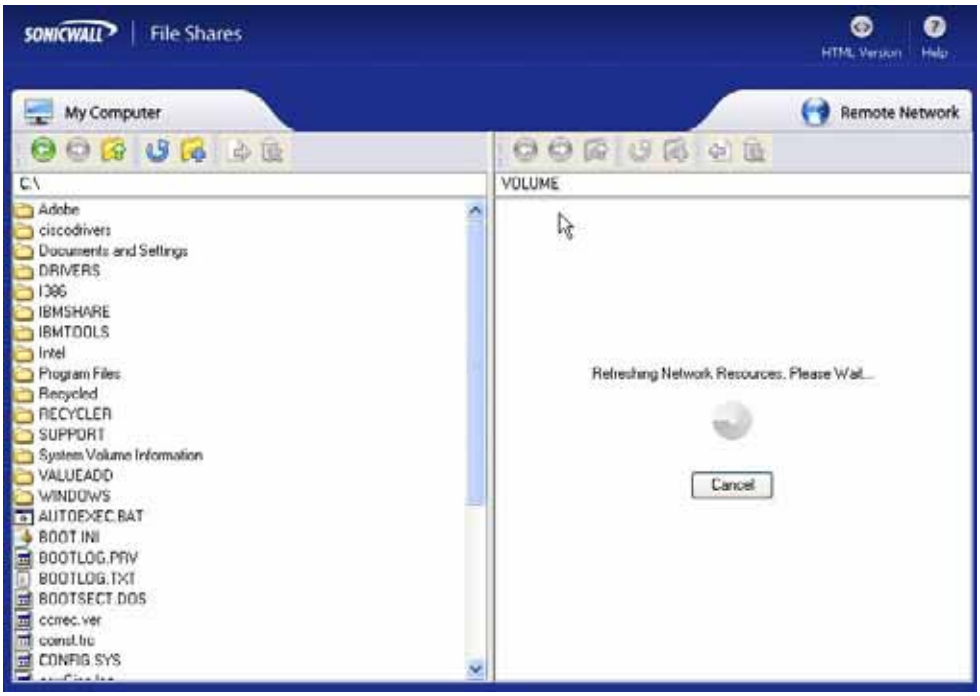
Windows Internet Explorer
Warning, you may not be running the optimal browser and Java Version for this product. Some features may not be available while running the File Shares Java Applet from this machine. Click OK to continue.
OK
Cancel

Note To avoid this warning, upgrade browser to Internet Explorer 6 or newer, Firefox 1.5 or newer, Opera 8 or newer, or Safari RSS. Also updates to Java 5.0 Update 10 or newer are recommended.

Step 4 Depending on the networks configurations and browser, one or more security warnings may display, click **Yes** or **Run** to continue.

Warning - Security
Do you want to accept the certificate from web site "sslvpn.eng.sonicwall.com" for the purpose of exchanging encrypted information?
Publisher authenticity can not be verified.
The security certificate was issued by a company that is not trusted.
The security certificate has not expired and is still valid.
More Details
Yes
No
Always

The File Shares Applet displays.

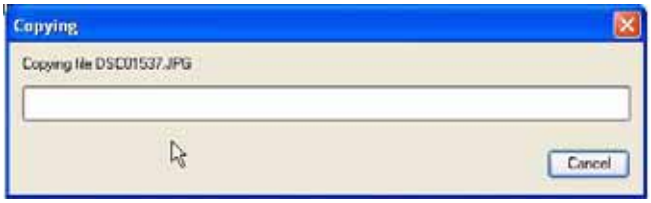


Note The File Shares Applet window will not automatically refresh when its contents have changed or if it has been previously viewed. To refresh, click the **Refresh** icon from the toolbar, or use the **Refresh** option from the right-click menu.

Note The remote network can be browsed from the remote window's address bar. The local directory can not be changed from the address bar. The remote path is capped at 1024 characters. The actual maximum string size will change depending on language.

Step 5 To select multiple items, click the items while holding the **shift** or the **ctrl** key. Clicking on an item again will de-select it and remove it from the group.

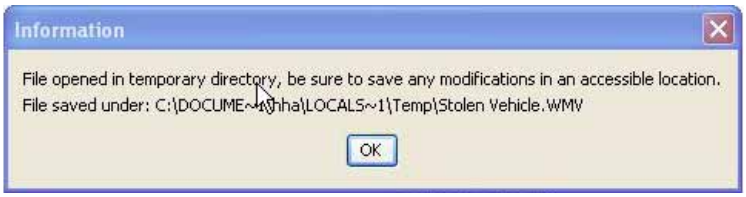
Step 6 To copy a file or group of files either to or from the network, select desired items and **click-and-drag** them across the center boundary. This will copy the file(s) into the open directory. Alternatively, the file(s) can be copied directly into a folder by dragging the icon and dropping over the desired folder; one could also use the **copy** button on the toolbar, or use the copy option from the right-click menu. A progress bar displays the waiting time required to copy the files.



Note The File Shares Applet supports overwriting existing files. If a file exists with the same name as the one you are trying to copy over, the Applet will prompt you to rename the file being copied. If the name is kept the same, the copied file will overwrite the existing one.

Step 7 **Double click** on a file to launch it with the proper application. If activating a file on the remote machine, the File Shares Applet will first download the file to a temporary folder on your machine and then open it.

Note The File Shares Applet will not always be able to delete the temporary file after use. Use caution when opening files with sensitive material.


Information
File opened in temporary directory, be sure to save any modifications in an accessible location.
File saved under: C:\DOCUME~1\hha\LOCALS~1\Temp\Stolen Vehicle.WMV
OK

File Shares Applet Browser Overview

Each window, local and remote, contains a set of buttons for commonly used operations in the toolbar. Hovering the mouse cursor over these icons displays convenient tool tips to the user. Dragging the toolbar by the dotted line on the left side of it undocks the toolbar into its own window. To re-dock the toolbar, close the window. These are the same functions as those in the right-click menu.

Here is a list of the buttons on the task bar and their respective function.

- **Back**: Traverses back in the history. Sets the current view of the window to the previous location in history. This icon is dimmed if there is no previous history location.
- **Forward**: Traverses forward in history. This icon is dimmed if there are no forward locations in history.
- **Up**: Traverses up the directory tree to the parent directory of the current view. This icon is dimmed if the current view is of the root directory or if the parent directory cannot be resolved.
- **Refresh**: Refreshes the current view by either polling the local file system or remote network via the SSL VPN. The refresh icon will be dimmed in the remote window if its contents are currently being refreshed.
- **New Folder**: Creates a new folder within the respective file system. Clicking this icon displays the “New Folder” dialog box, allowing the user to assign a name to the new folder. This icon is dimmed when the location of the window is such that a new folder cannot be created. (for example, Root of a Windows filesystem, domain list, machine list).
- **Copy**: Copies the selected file(s)/folder(s) to the location of the remote window. Clicking this icon displays the “Copy” dialog box that will show the status information of the copy procedure. If the file being copied already exists, a new dialog will display asking the user whether or not the existing file should be replaced. The copy icon is dimmed when there are no selected files/folders to copy (for example, if no drive or domain is selected). It is also dimmed if the remote location cannot accept files copied to it (for example, Domain List/ Machine List). Copying a folder also copies everything within the folder.

- **Delete**: Deletes the selected file(s)/folder(s). Deleting a folder will delete everything within the folder.

Note Files deleted this way are fully removed from the original machine they were on. These files are not sent to the recycling bin and are in no way recoverable.

Configuration Examples

The following configuration examples provide a demonstration of the usefulness and flexibility of the File Shares Applet.

- Configuring Bookmarks from Within the File Shares Applet, page 76
- Using Bookmarks from Within the File Shares Applet, page 78
- Moving Files and Folders, page 78
- Launching a File Directly from the File Shares Applet, page 82

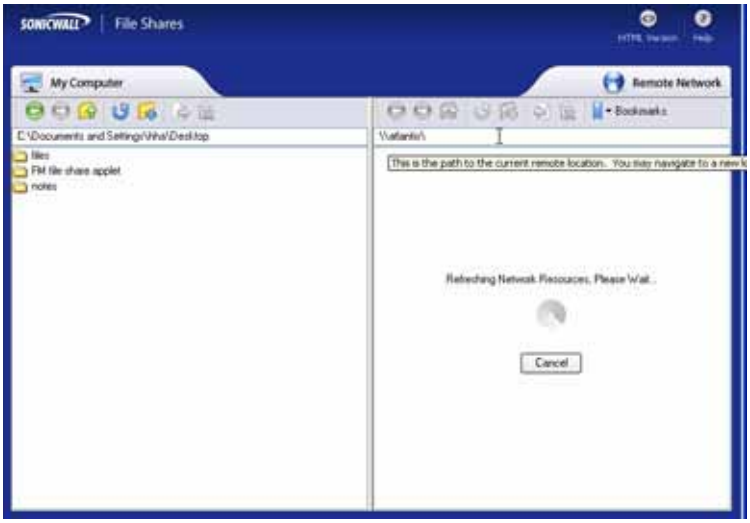
Configuring Bookmarks from Within the File Shares Applet

Navigating a remote computer's directory hierarchy structure takes a long time. To reduce this process as much as possible, the SonicWALL SSL VPN File Shares Applet allows the user to create bookmarks on the fly from within the File Shares Applet itself. This allows the user to skip the hierarchy structure of the remote computer the next time she needs to access a particular file or folder.

Step 1 Launch the File Shares Applet by clicking on the **File Shares** button in the Virtual Office portal. The File Shares Applet displays.

Step 2 The File Shares Applet's default location for the local window is the base directory, while the remote window shows the entire network. Double click on the appropriate folders to navigate the local window to the desktop or another appropriate folder.

Step 3 To navigate the remote window, double click on a visible computer, or input the name in the address bar preceded by **** and followed by a **** and press **Enter.** The File Shares Applet will then navigate to the requested computer. It may take several seconds for the resources to load, depending on the network configuration.

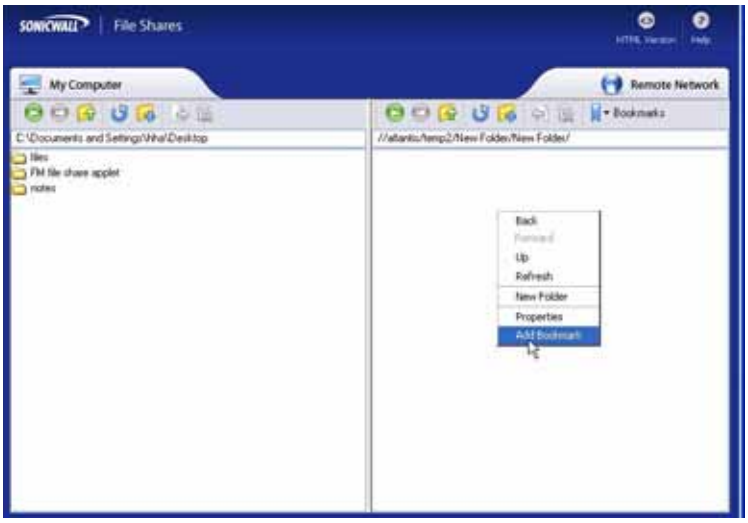


Step 4 Once loaded, double click on a folder or enter the target directory path within the address bar. This can take some time as the File Shares Applet must browse through the network after every change.

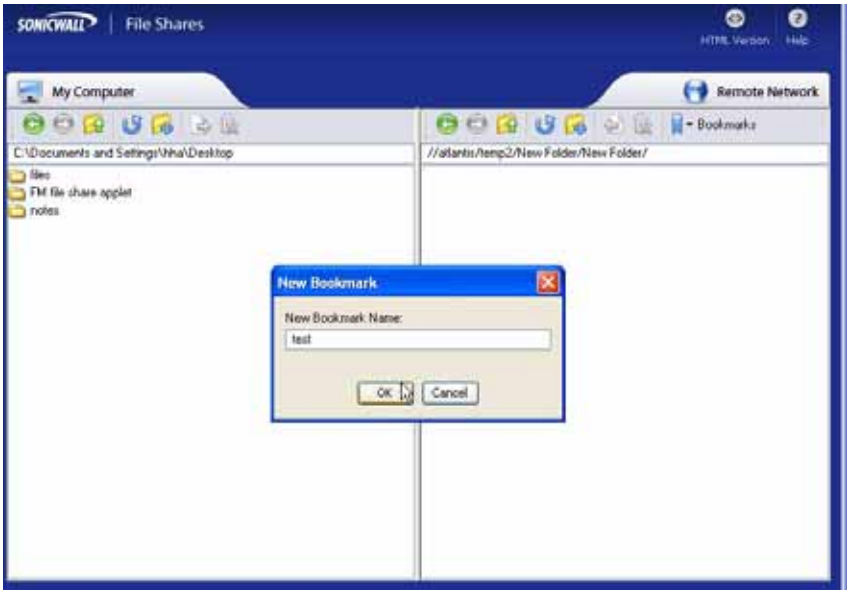
Note Only the remote window can use the address bar to navigate through a computer's file hierarchy.

Step 5 To set a bookmark to the current directory, right-click in an empty location in the remote directory and select **Add Bookmark**.

Note To set a bookmark for a specific file or folder, select it prior to selecting **Add Bookmark** from the right-click menu.



Step 6 Enter a name for the new bookmark in the New Bookmark window that displays.



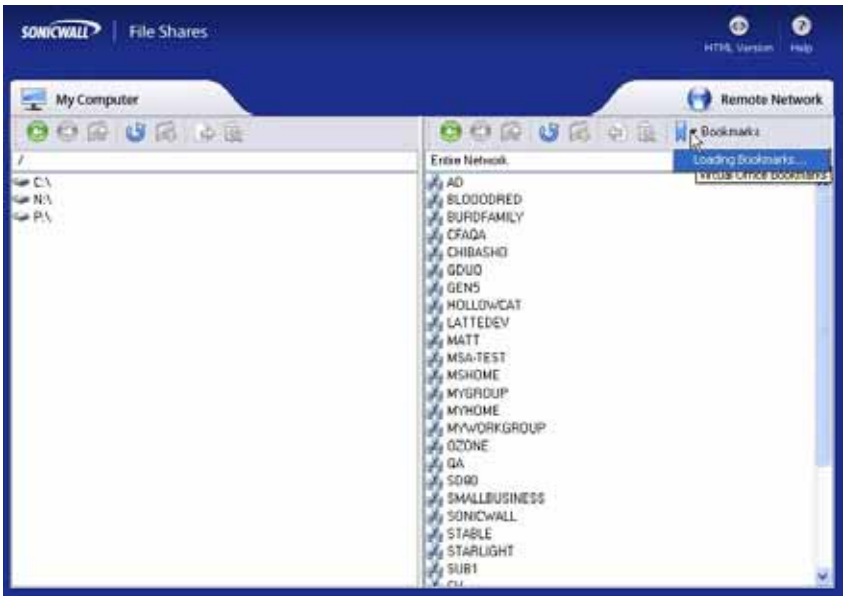
Step 7 Click **OK**. The bookmark is added to the Virtual Office portal. Clicking on the bookmark accesses the selected folder or file.

Using Bookmarks from Within the File Shares Applet

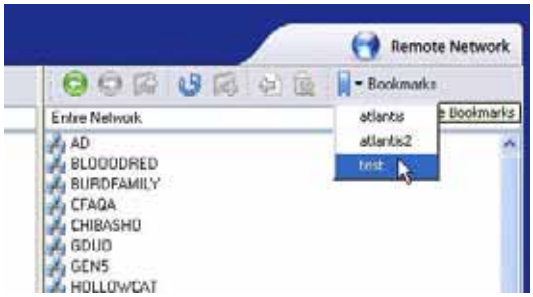
In Addition to accessing bookmarks from the Virtual Office portal, bookmarks can be easily accessed from within the File Shares Applet.

Step 1 Launch the File Shares Applet by clicking on the **File Shares** button in the Virtual Office portal.

Step 2 Click on the **Bookmarks** button on the task bar in the remote window. A pull down menu displays with the message **Loading Bookmarks**. Keep the mouse within the pull down menu as the File Shares Applet loads the bookmarks.



Step 3 Once loaded, click book mark to load the desired file or folder.



Moving Files and Folders

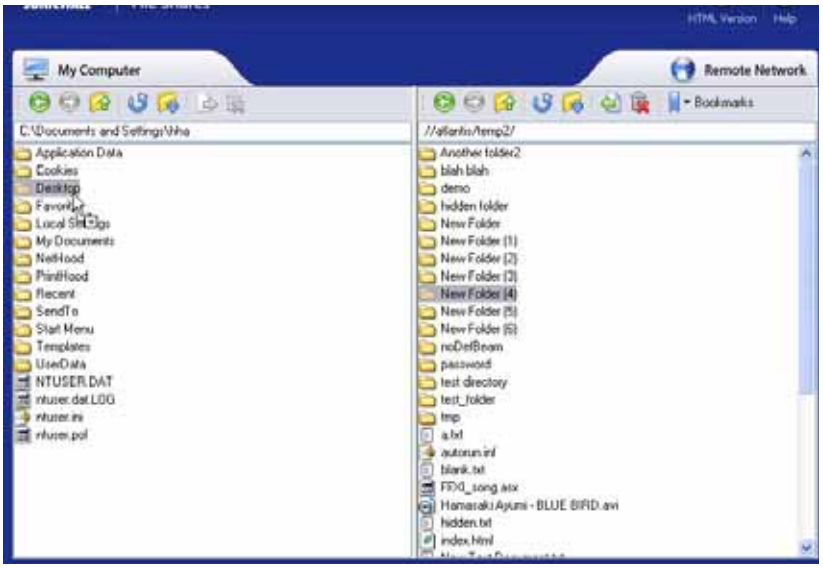
The File Shares Applet is designed for ease of use. There is more than one way to perform file transfers.

This section provides an example of a folder that is copied from a remote machine onto the local machine's desktop, deleted from the remote machine, and moved back from the local machine unto the remote machine, all from the File Shares Applet.

Step 1 Launch the File Shares Applet by clicking on a bookmark in the Virtual Office portal.

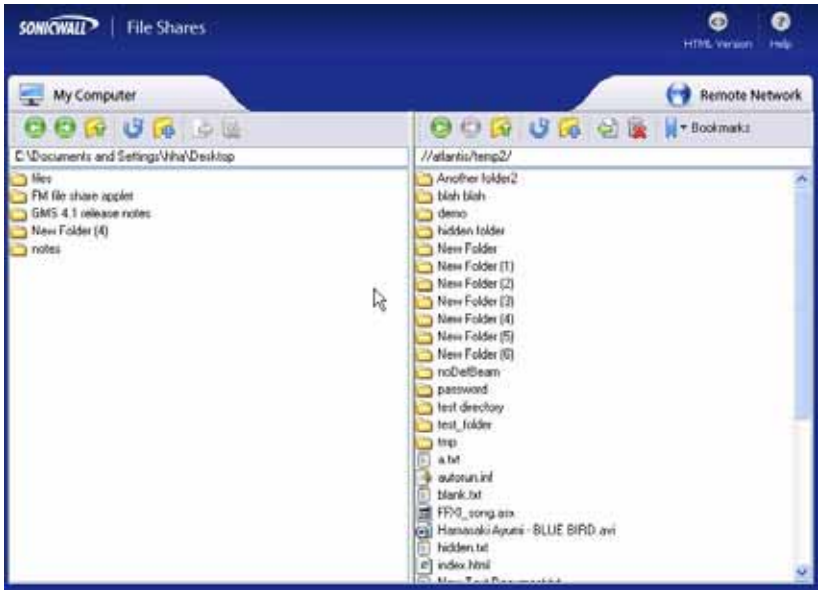
Step 2 Double-click the **C:** drive, double-click the **Documents and Settings** folder, then double-click a specific folder, for example, the one that holds the **Desktop** folder.

Step 3 The current directory shows the **Desktop** folder. Select a file or folder from the remote machine and drag its icon onto the **Desktop** folder in the local machine. This will copy the item from the remote machine directly onto the desktop.



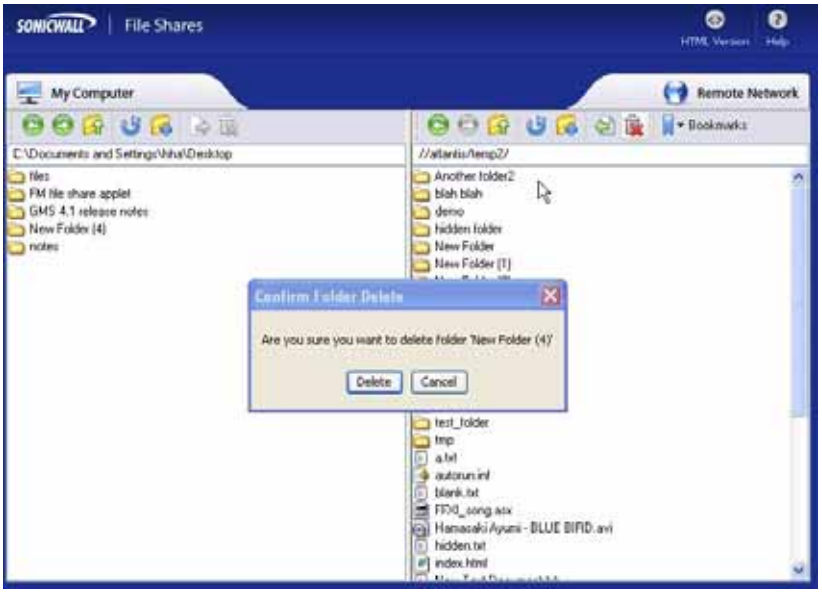
Step 4 Once the transfer is complete, double-click on the **Desktop** folder. The folder copied from the remote machine will display in that folder.

Note The item still exists on the remote machine. To initiate a move, not a copy, you must use the **Move** command from the right-click menu.



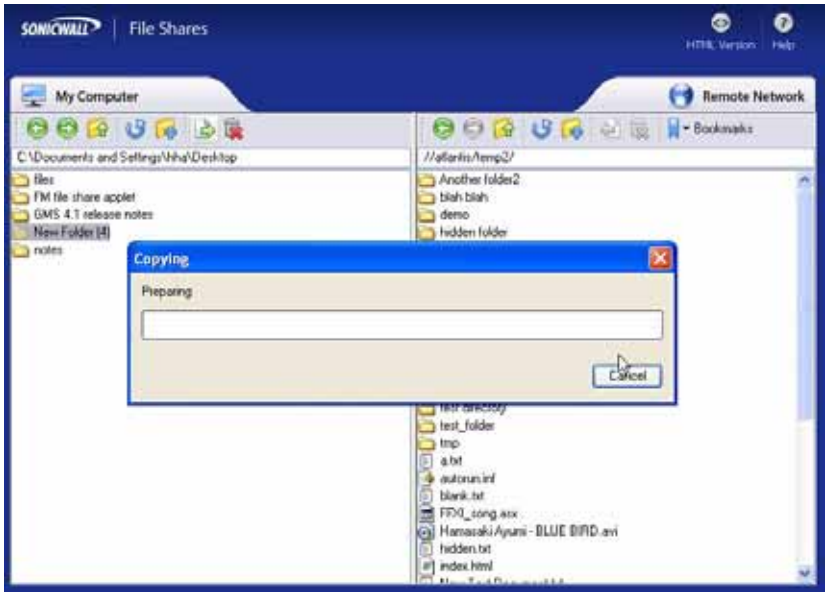
Step 5 To delete the original file or folder, select it by clicking on it once, and press the **Delete** button on the tool bar. Alternatively, the item can be deleted by using the right-click menu. The File Shares Applet displays a delete confirmation window. Click the **Delete** button in the pop-up to delete the item.

Warning **The File Shares Applet will completely delete the file or folder from the remote machine. In the case of a folder, nested items will also be deleted. These items will not be sent to the recycle bin on either machine and are not recoverable.**



Step 6 Once the file or folder has been deleted, the File Shares Applet will automatically refresh, removing the item from the current directory. To copy it from the local machine back to the remote machine, click-and-drag like in **Step 2**, or use the **Copy** icon from the local machine's tool bar.

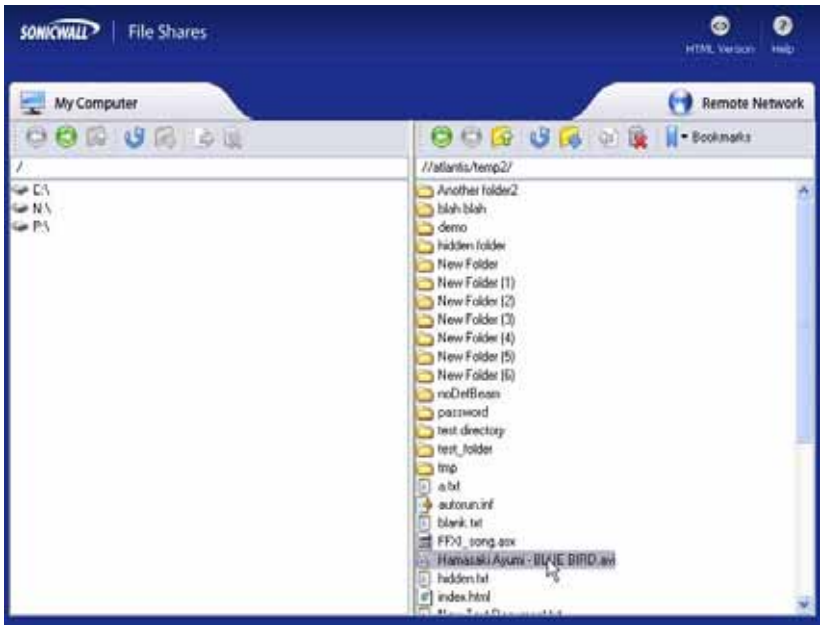
Note The **Copy** icon in the toolbar automatically moves the selected file to whatever directory is currently open. To move an item to a different folder, either drag-and-drop it into the desired destination or open the desired destination prior to clicking **Copy**.



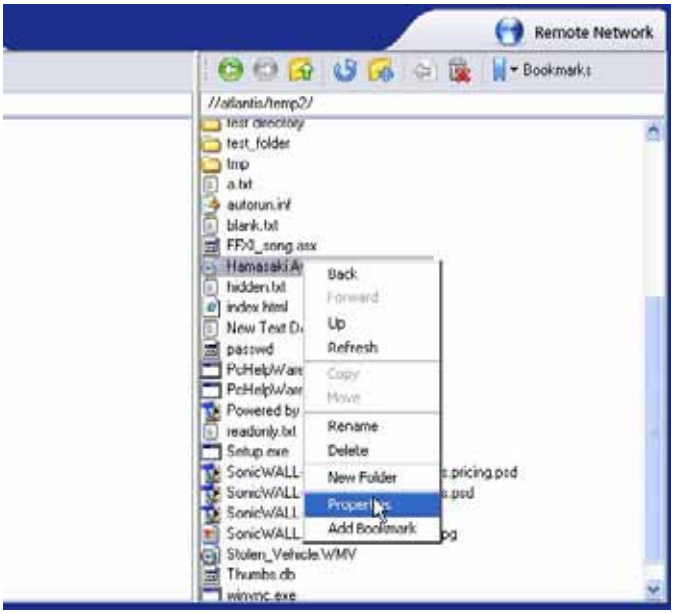
Launching a File Directly from the File Shares Applet

Files can be launched from within the File Shares Applet. This section provides an example where a remote file is queried for its properties, bookmarked and opened.

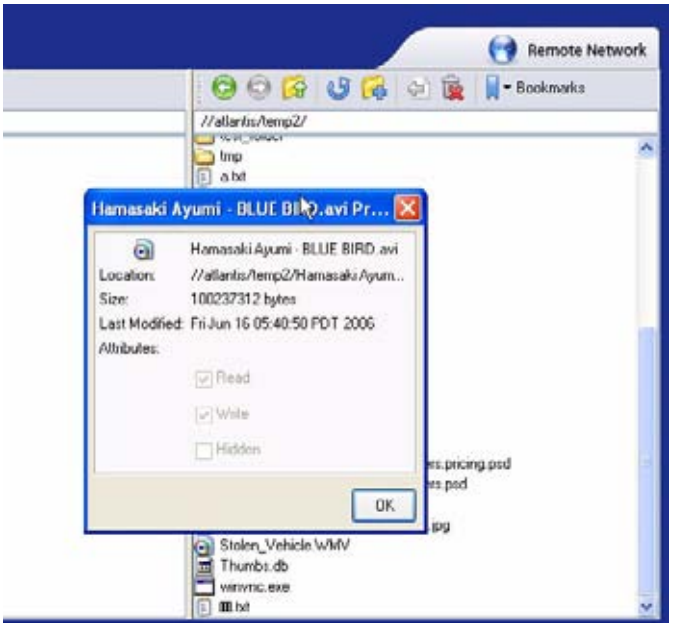
Step 1 Launch the File Shares Applet by clicking on a bookmark in the Virtual Office portal.



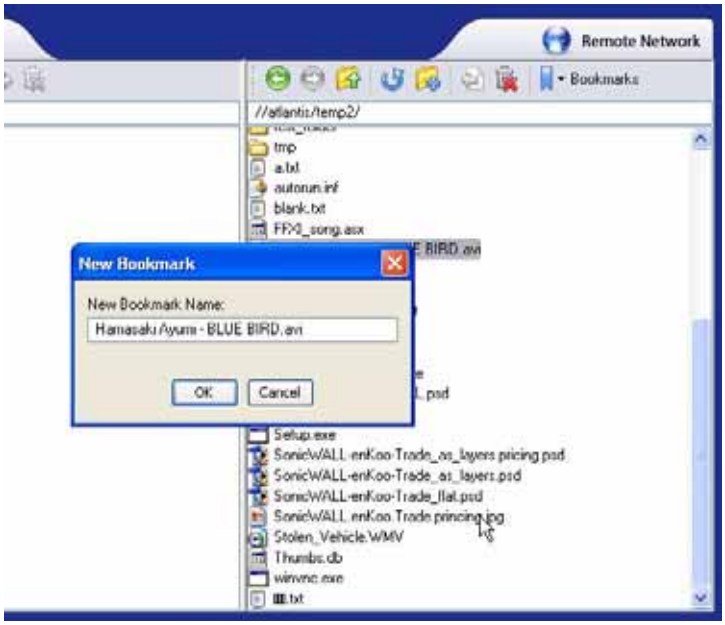
Step 2 Right click the file and select **Properties**.



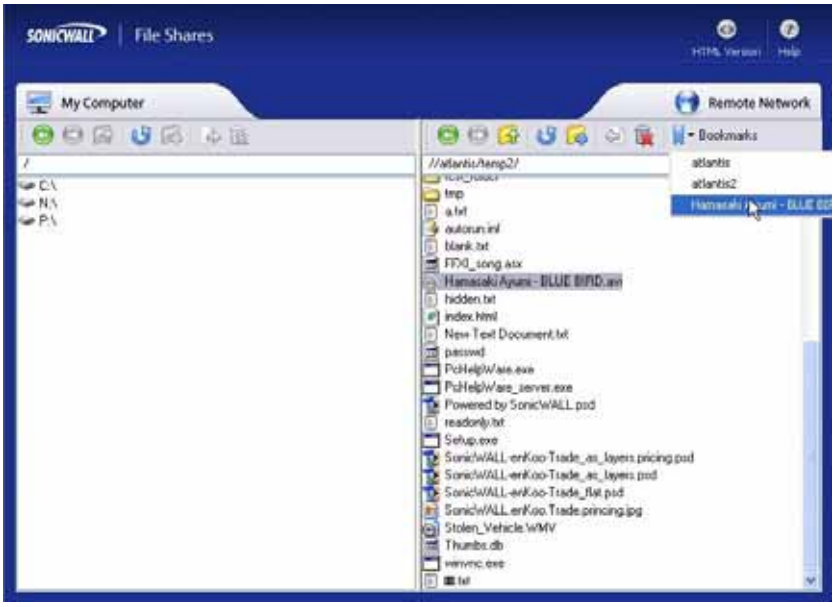
The file's properties will be displayed in a separate window.



Step 3 To open the file, double-click on the file. Alternatively, create a bookmark to it, and launch the file from the bookmark menu. To create a bookmark, select the **Add Bookmark** option from the right-click menu. The name of the file is the default name of the new bookmark, but a new name can be entered if so desired.



Step 4 Then select the bookmark, either from the portal or from the bookmark tab in the toolbar.



Note Files launched from within the File Shares Applet must be downloaded to the local machine before they can be opened. The File Shares Applet will store the file in a temporary directory while it is being used. The File Shares Applet will also try to delete the file after use, but may be unable to do so depending on whether or not another program is accessing it. Use caution when opening files with sensitive material.

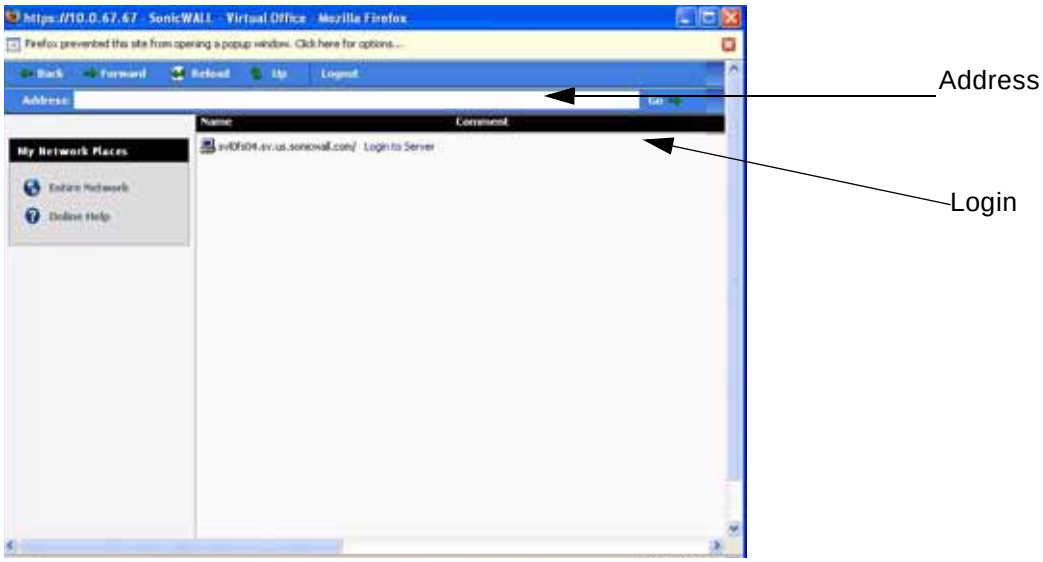
Using HTML-Based File Shares

File shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

Note The server can be specified either by name or by IP address, for example, **\\moosedc** or **\\10.50.165.2**. For names to work, it is necessary that DNS and/or WINS be properly configured by the administrator on the SSL-VPN appliance to be able to resolve host names.

To create a file share, perform the following steps:

Step 1 Click on the **File Shares** button. Virtual Office displays a dialog box that provides a hot link to a login prompt.



Note Pop-up window blockers may prevent File Shares from functioning properly. Configure your browser to allow pop-up windows on the SSL VPN portal site.

Step 2 To specify a new share path (as an example, **\\moosedc**) in the **Address** field. You need to precede the share name with two back slashes. For example: **\\file-directory01.example.com**.

Step 3 To connect to a pre-existing file share, click the **Login to Server** link next to the file share name.

Step 4 Click the **go** prompt to display the **Enter Network Password** dialog box.

Step 5 Type a valid username in the User Name field and a valid password in the Password field and click **Login**.

Step 6 Virtual Office displays the home File Share screen that you have specified, displaying folders on the network to which you can navigate.

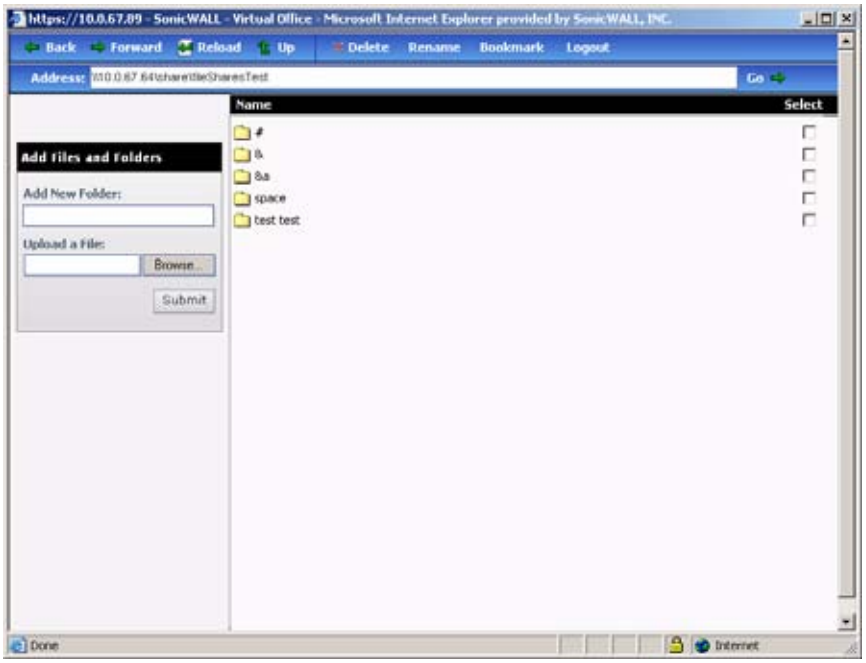


Table 2 describes the controls at the top of the File Share window.

Table 2 File Share Controls

Button	Description
Back	Navigate to the previous File Share location.
Forward	Navigates forward to the previous File Share location after you have pressed the **Back** button.
Reload	Reloads the current folder to display any changes.
Up	Navigates
Delete	Deletes the selected folders and files. Select items by checking the checkbox next to their name under the **Select** column.
Rename	Renames the selected folders and files. Select items by checking the checkbox next to their name under the **Select** column.
Bookmark	Creates a new bookmark to the current File Share location.
Logout	Logout of the File Share service.

Step 7 You can now navigate the folders and files in the File Share as you would through Windows Explorer or other file management systems.

Step 8 To add a new folder in the current File Share location, type the name of the folder in the **Add New Folder:** field and click **Submit**.

Step 9 To add a file in the current File Share location, click the **Browse...** button. Navigate to the location of the file on your computer in the **Choose file** window that opens, select the file and click **OK**, and then click **Submit** in the File Share window.

Managing Bookmarks

Bookmarks are objects that enable you to connect to a location or application conveniently and quickly. The Virtual Office Bookmark system allows bookmarks to be created at the group and user levels. The administrator can create both group and user bookmarks which will apply to applicable users while individual users can create only personal (user-level) bookmarks.

Since bookmarks are stored within the security appliance's local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local groups and users (LocalDomain), this is automated since the administrator must manually define the groups and users on the device. Similarly, when working with external groups (not LocalDomain), the correlation is automated since creating an external domain creates a corresponding local group.

However, when working with external users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SSL-VPN's configuration files. The need to store bookmarks on the SSL-VPN itself is because LDAP, RADIUS, and NT authentication external domains do not provide a direct facility to store such information as bookmarks.

Rather than requiring administrators to manually create local users for external domain users wishing to use personal bookmarks, SonicWALL SSL VPN automatically creates a corresponding local user entity when an external domain user logs in to the Virtual Office.

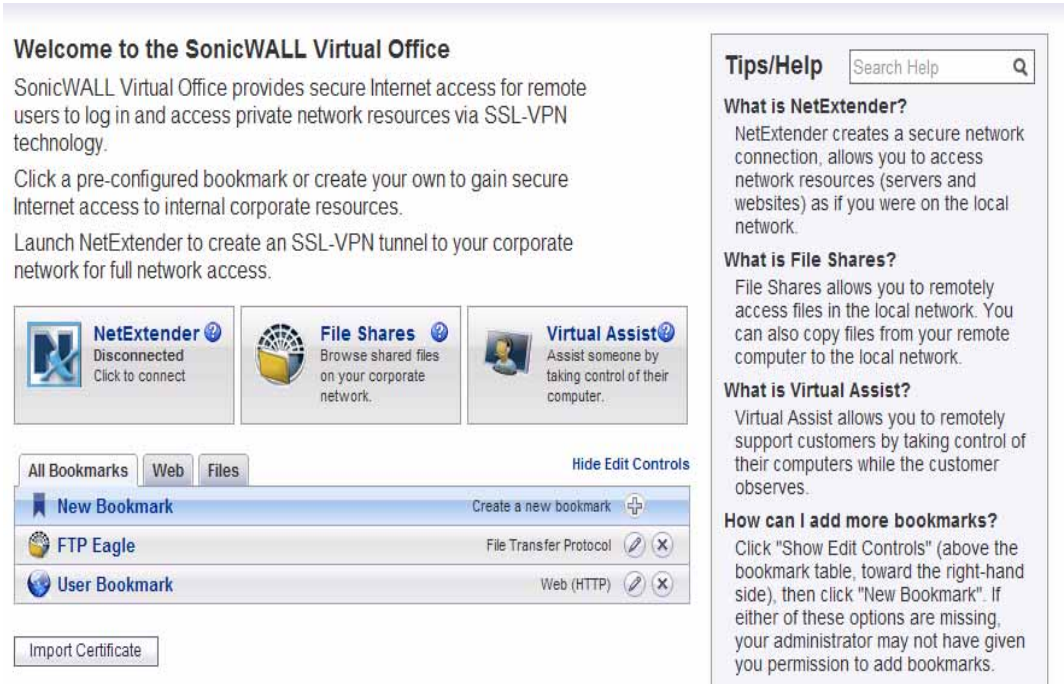
The following sections describe basic bookmark tasks:

- "Adding Bookmarks" section on page 88
- "Editing Bookmarks" section on page 92
- "Removing Bookmarks" section on page 93

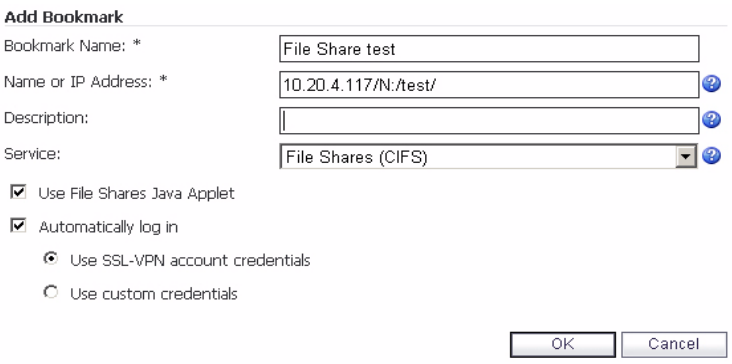
Adding Bookmarks

Bookmarks provide a convenient way for you to access Web, FTP, or other services on the remote network that you will connect to frequently. To define bookmarks, perform the following:

Step 1 From the Virtual Office window, click **Add Bookmark** in the Bookmarks table. An Add Bookmark window will be displayed.


Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Virtual Assist
Assist someone by taking control of their computer.
All Bookmarks
Web
Files
Hide Edit Controls
New Bookmark
Create a new bookmark
FTP Eagle
File Transfer Protocol
User Bookmark
Web (HTTP)
Import Certificate
Tips/Help
Search Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.
What is Virtual Assist?
Virtual Assist allows you to remotely support customers by taking control of their computers while the customer observes.
How can I add more bookmarks?
Click "Show Edit Controls" (above the bookmark table, toward the right-hand side), then click "New Bookmark". If either of these options are missing, your administrator may not have given you permission to add bookmarks.

Step 2 Enter a descriptive name in the **Bookmark Name** field.



Step 3 Enter the domain name, IP address, or IPv6 address of a host machine on the LAN in the **Name or IP Address** field. IPv6 addresses should be enclosed in brackets (i.e. the [and] symobls).

Step 4 Select the service type in the Service menu. You can select from the following services:

- Terminal Services (RDP - ActiveX)
- Terminal Services (RDP - Java)
- Virtual Network Computing (VNC)
- File Transfer Protocol (FTP)
- Telnet

- Secure Shell version 1 (SSHv1)
- Secure Shell version 2 (SSHv2)
- Web (HTTP)
- Secure Web (HTTPS)
- File Share (CIFS/SMB)
- Citrix Portal (Citrix)

Step 5 For Citrix bookmarks, you can optionally designate that it be a secure Citrix connection by checking the **HTTPS Mode** checkbox.

Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this checkbox leverages this portability.

Step 6 For RDP - ActiveX, RDP - Java and FTP, select the box next to **Use SSL-VPN account credentials to log in** to use SSL VPN account credentials to log in. Leave the box unchecked to use custom credentials for each bookmark login.

Step 7 For SSHv2, you must have SUN JRE 1.4 or 1.5 and must be connecting to a server that supports SSHv2. There are also options to **Automatically accept host key** and to **Bypass username**. The bypass option should only be used for SSHv2 servers that do not require authentication in the initial connection session (such as SonicWALL security appliances).

Step 8 For HTTP(S) bookmarks, you can select **Use SSL-VPN account credentials to log in** or configure custom credentials for use with Single Sign-On. To disable the use of SSO, clear the **Automatically log in** checkbox.

Step 9 Click **Add** to add the bookmark.

Once the configuration has been updated, the new bookmark will be displayed in the Virtual Office Bookmarks table. Click on a bookmark description to go to the bookmark location that you have defined.

Configuring RDP ActiveX and Java Bookmarks

ActiveX and Java RDP bookmarks offer several features that are not available in other bookmarks.

Tip The ActiveX client is only supported on the Internet Explorer browser, while the Java client is supported on all platforms and browsers that are compatible with SonicWALL SSL VPN.

Step 1 Enter the desired **Bookmark Name**.

Step 2 Enter the **Name or IP Address** of the resource you are trying to reach. You can also use an IPv6 address.

Step 3 Select **Terminal Services (RDP - ActiveX)** or **Terminal Services (RDP -Java)** from the **Services** list.

Step 4 Continue to configure the RDP ActiveX or Java Bookmark as follows:

Option	Usage
Screen Size	Select the default screen size to be used when users execute this bookmark. It is advised that you select a size equal to or smaller than your current desktop screen size. ActiveX RDP bookmarks also have a **full-screen** option that will display the RDP window in full screen mode. To toggle from the RDP window back to your desktop, press **Alt-Tab**.
Colors	Select the default color depth to be used when users execute this bookmark.
Application and Path	To have the RDP session launch an application when the bookmark is initiated, enter the path to the application in the **Application and Path (optional):** field. For example, **C:\Program Files\Example\app.exe** (optional).
Start in the following folder	Enter the local folder to execute application commands in (optional).
Login as console/admin session	Check this option to enable console and admin commands on login.

Option	Usage
Enable Wake on LAN	Select this option to send WoL packets to the host. This option also allows entering one or more **Mac Address**es (separated by spaces) for the machines to wake and the desired **Wait time for boot up** before cancelling the WoL operation. To send the WoL packet to the hostname or IP of this bookmark, check the **Send WOL packet to bookmark host Name or IP address** checkbox, this option can be applied in tandem with a Mac address.
Redirects (ActiveX only)	Optionally expand **Show windows advanced options** and select any of the redirect checkboxes **Redirect printers**, **Redirect drives**, **Redirect ports**, or **Redirect smartCards** to redirect those devices on the local network for use in this bookmark session.
Redirects (Java only)	Optionally expand **Show windows advanced options** and select any of the redirect checkboxes **Redirect printers**, **Redirect drives**, **Redirect ports**, **Redirect smartCards**, **Redirect clipboard** and **Redirect plug and play devices**, as well as any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/ window animation**, **Themes**, or **Bitmap caching**. If the client application will actually be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, and **Remote Application**.
Enable Plugin Dlls (ActiveX only)	Enter the name(s) of client DLLs which need to be accessed by remote the desktop or terminal service. Multiple entries are separated by a comma "**,**" with no spaces. Make sure any DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32). Note: The RDP - Java client is a native RDP client and supports Plugin DLLs by default.
Automatically log in	Check this option and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark.

Tip The ActiveX client is only supported on the Internet Explorer browser, while the Java client is supported on all platforms and browsers that are compatible with SonicWALL SSL VPN.

Step 5 When you are finished. Click the **Add** button to add this bookmark to your Virtual Office list.

Determining the Remote Computer's Full Name or IP Address

Complete the following steps to determine the full name of the computer to which the RDP bookmark is pointing:

Step 1 Right click on the **My Computer** icon on the desktop of the remote computer, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 The full computer name will be listed under Remote Desktop.

Complete the following steps to determine the IP address of your computer.

Step 1 In the Windows **Start** menu on the remote computer, navigate to **Run...**

Step 2 Type **cmd** to open the command interpreter and click **OK**.

Step 3 Type **ipconfig**. The IP address of your computer is displayed.

Configuring Remote Desktop Access on the Remote Computer

Complete the following steps to allow remote desktop access to the computer that is the target of the RDP bookmark:

Step 1 Right click on the **My Computer** icon on the desktop, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 Under Remote Desktop, select the checkbox for **Allow users to connect remotely to this computer**.

Step 4 Click **OK**.

Editing Bookmarks

You can change the IP address, domain name, or IPv6 address as well as the service and other settings associated with an existing bookmark.

Note Only user-created Bookmarks can be edited or deleted by the user. Global or Group Bookmarks pre-defined by the administrator cannot be edited or deleted.

To edit a bookmark to change its name or associated IP address, perform the following steps:

Step 1 Identify a bookmark in the Virtual Office Bookmarks list for which you want to change an IP address or domain name or other settings.

Step 2 In the Virtual Office Bookmarks list, click on the Configure icon for an existing bookmark. The **Edit Bookmark** dialog box displays.

Step 3 To change the bookmark name, domain name or IP address of the bookmark, edit the names in the **Bookmark Name** or **Name or IP Address** fields.

Step 4 To change the service, select a new **Service** from the pull-down menu.

Step 5 Optionally change other settings specific to the **Service** type.

Step 6 Optionally enable or disable the **Automatically log in** setting, or change the credentials selection.

Step 7 Click **Apply**. The Virtual Office home page displays with the new IP address or domain name.

Removing Bookmarks

To remove a bookmark, perform the following steps:

Step 1 Identify a bookmark in the Virtual Office Bookmarks list that you want to remove.

Step 2 In the Virtual Office Bookmarks list, click on the delete icon for the bookmark you want to remove. The bookmark disappears from the list.

Caution No warning message is displayed after you click the delete icon. The bookmark will be deleted immediately.

Using Bookmarks

The following sections describe how to use the various types of bookmarks:

- "Using Remote Desktop Bookmarks" section on page 93
- "Using VNC Bookmarks" section on page 95
- "Using FTP Bookmarks" section on page 98
- "Using Telnet Bookmarks" section on page 101
- "Using SSHv1 Bookmarks" section on page 102
- "Using SSHv2 Bookmarks" section on page 103
- "Using HTTP and HTTPS Bookmarks" section on page 104
- "Using File Share Bookmarks" section on page 105
- "Using Citrix Bookmarks" section on page 105
- "Global Bookmark Single Sign-On Options" section on page 108
- "Per-Bookmark Single Sign-On Options" section on page 108

Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. SonicWALL SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by the SonicWALL SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag

- Menu/window animation
- Themes
- Bitmap caching

If the Java client application is RDP 6, it also supports:

- Dual monitors
- Font smoothing
- Desktop composition

Note RDP bookmarks can use a port designation if the service is not running on the default port.

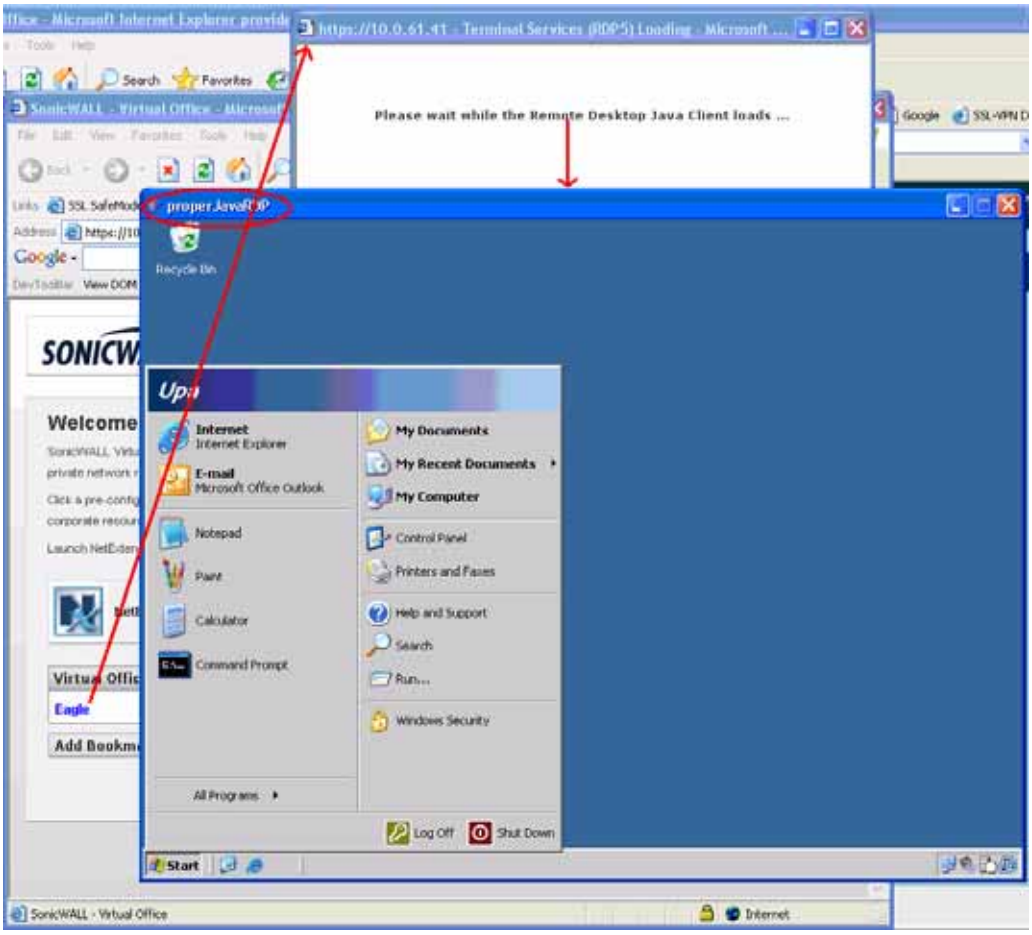
Tip To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

Step 1 Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **Ok**.

Warning - Security
The web site's certificate is invalid. Do you want to continue?
Name: 10.0.67.89
Publisher: 10.0.67.89
Always trust content from this publisher.
Yes
No
The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application.
More Information...

Step 2 Enter your username and password at the login screen and select the proper domain name from the pull-down menu.

Step 3 A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.



Note For information on configuring options for RDP bookmarks, see "Configuring RDP ActiveX and Java Bookmarks" on page 89.

Using VNC Bookmarks

Step 1 Click the VNC bookmark. The following window is displayed while the VNC client is loading.

Note VNC can have a port designation if the service is running on a different port.

Virtual Network Computing (VNC) - Microsoft Internet Explorer provided by So...
Please wait while the Virtual Network Computing Client loads ...
Click the Close window button to close this window after you are finished with your Virtual Network Computing session.
Close Window

Step 2 When the VNC client has loaded, you will be prompted to enter your password in the **VNC Authentication** window.

Step 3 To configure VNC options, click the **Options** button. The **Options** window is displayed.

Table 3 describes the options that can be configured for VNC.

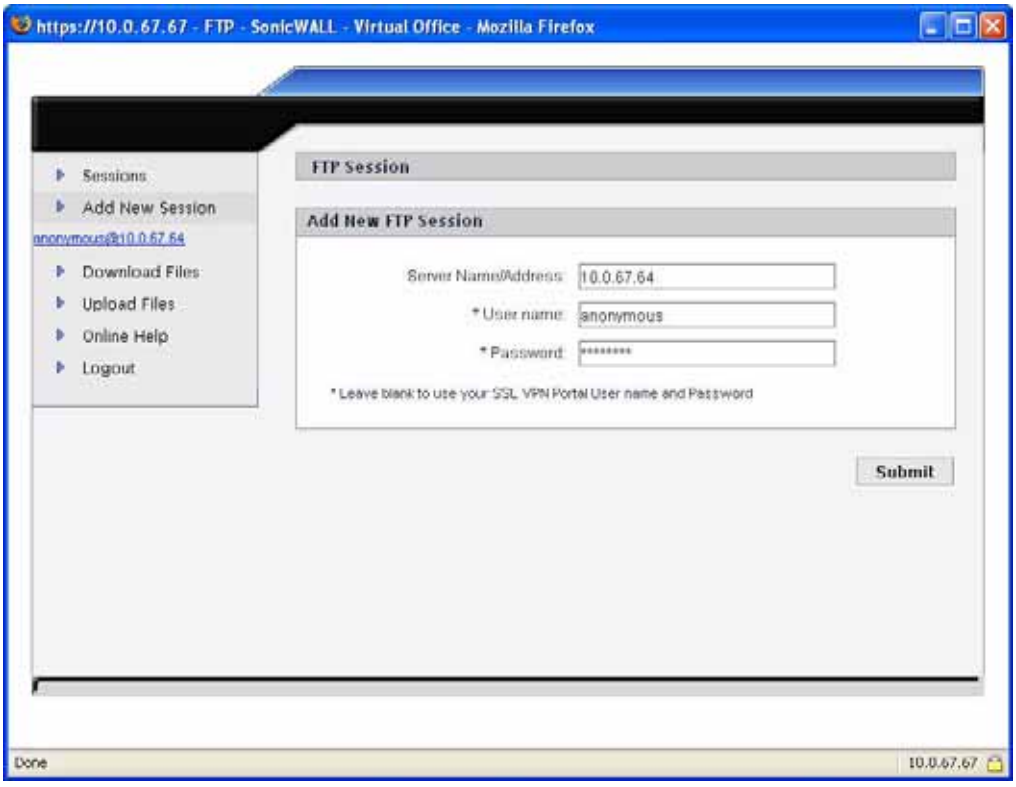
Table 3 VNC Options

Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG image quality	6	This cannot be modified.
Cursor shape updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable** but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.
Mouse buttons 2 and 3	Normal	If set to **Reversed**, the right mouse button (button 2) will act as if it was the middle mouse button (button 3), and vice versa.
View only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.
Share desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No** then an existing user session will end when a new user accesses the desktop.

Using FTP Bookmarks

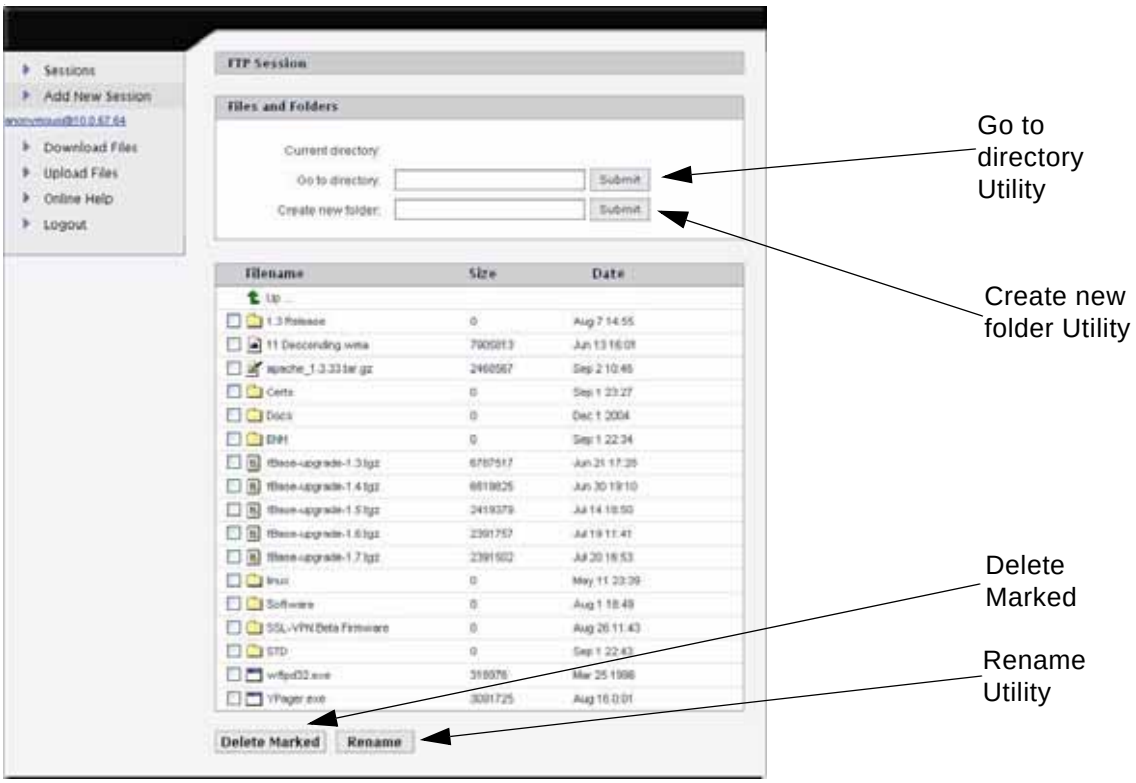
Note FTP bookmarks can use a port designation if the service is not running on the default port.

Step 1 Click the **FTP** bookmark. The **FTP Session** dialog box displays.



Step 2 Enter your username and password. If you want to use your Virtual Office username and password, simply leave the fields blank.

Step 3 Click **Submit**. An FTP session displays.



Step 4 You can use the following utilities in the FTP site:

- To manually navigate to a folder, enter the folder name in the **Go to directory** field and click **Submit**.
- To create new folders in the directory, use the **Create new folder** fields.
- To delete multiple files, click in the checkboxes of files or folders you want to remove and click **Delete Marked**.
- To rename a file or folder, click in the checkbox of a file or a folder and click **Rename**.

Step 5 To initiate another FTP session, click the **Add New Session** button. To return to the initial FTP session, click the link for it (in the form username@ipaddress) under the **Add New Session** button.

Downloading Files

To download a file, perform the following:

Step 1 Click **Download Files** in the navigation bar.

Step 2 Click on the name of the file in the **Filename** column. The File Download window displays.

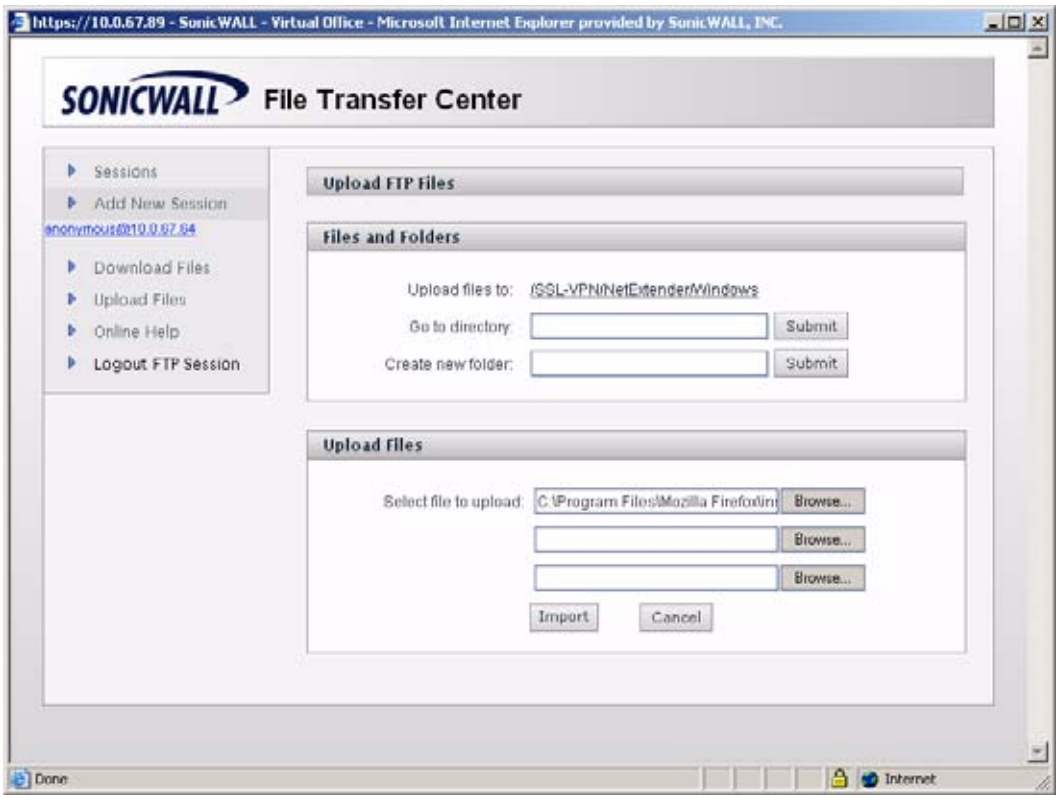
File Download - Security Warning
Do you want to run or save this file?
Name: NetExtender[1].Windows.1.0.2.setup.exe
Type: Application
From: 10.0.67.89
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Step 3 Click **Run** to launch the file. Click **Save** to save it to your computer.

Uploading Files

To upload a file, perform the following:

Step 1 Click **Upload Files** in the navigation bar. The Upload FTP Files window will be displayed.



Step 2 The current directory is displayed in the **Upload files to:** field. To navigate to a different directory, enter the directory name in the **Go to directory:** field. To create a new folder in the current directory, enter the name of the folder in the **Create new folder:** field and click submit.

Step 3 Select the file you want to upload by clicking the **Browse...** button and navigating to the file. You can upload up to three files at once.

Note To navigate between uploads, click the **Sessions** link.

Step 4 Click **Import** to upload the files.

Using Telnet Bookmarks

Step 1 Click on the Telnet bookmark.

Note Telnet bookmarks can use a port designation for servers not running on the default port.

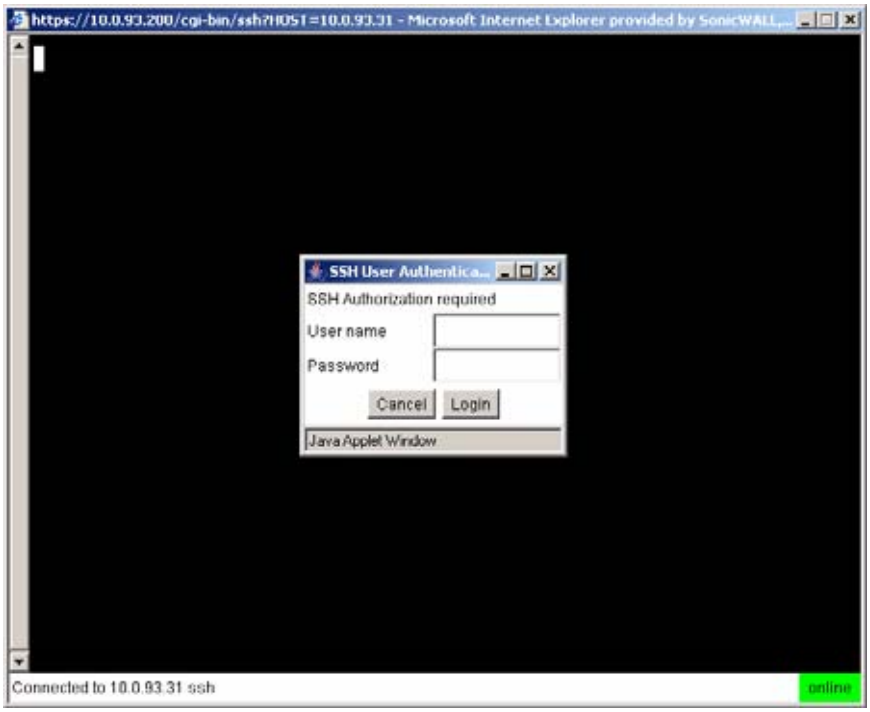
Step 2 Click **OK** to any warning messages that are displayed. A Java-based Telnet window launches.

Step 3 If the device you are Telnetting to is configured for authentication, enter your username and password.

Using SSHv1 Bookmarks

Note SSH bookmarks can use a port designation for servers not running on the default port.

Step 1 Click on the SSHv1 bookmark. A Java-based SSH window is launched.



Step 2 Enter your username and password.

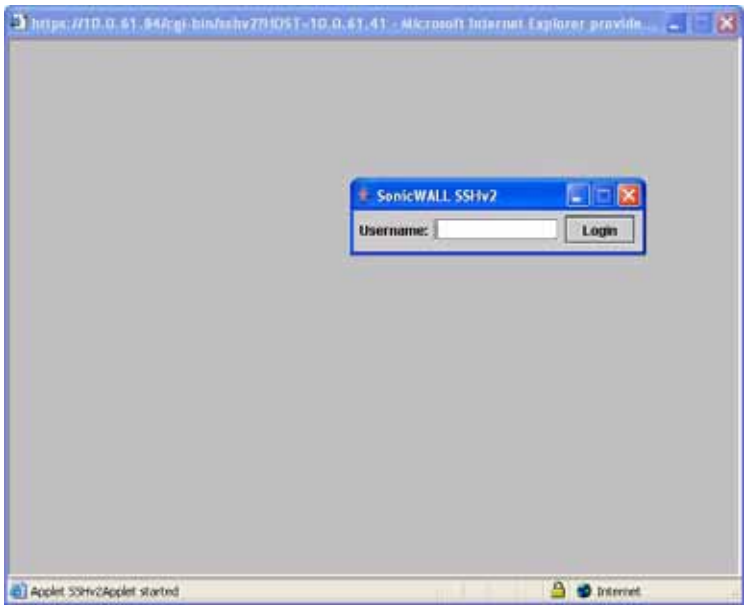
Step 3 A SSH session is launched in the Java applet.

Tip Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

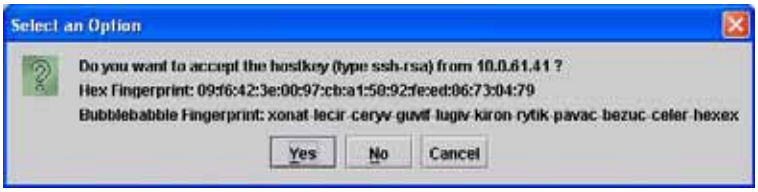
Using SSHv2 Bookmarks

Note SSH bookmarks can use a port designation for servers not running on the default port.

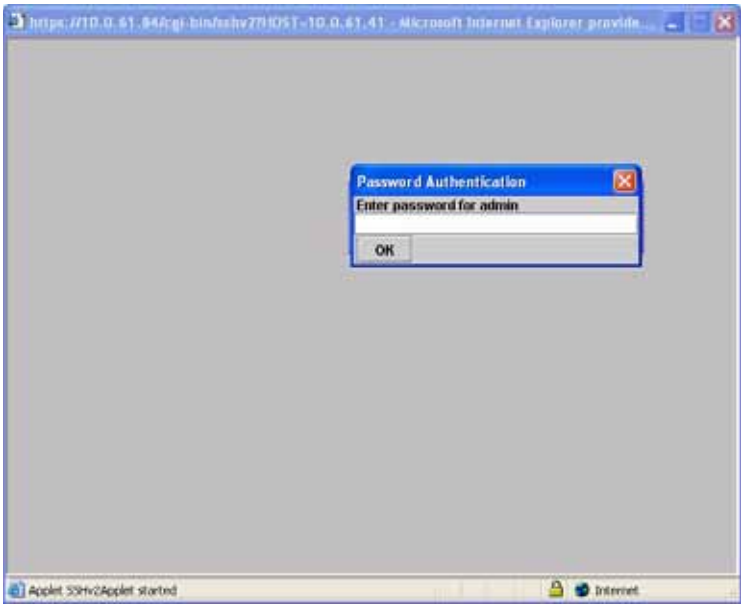
Step 1 Click on the SSHv2 bookmark. A Java-based SSH window displays. Type your user name in the **Username** field and click **Login**.



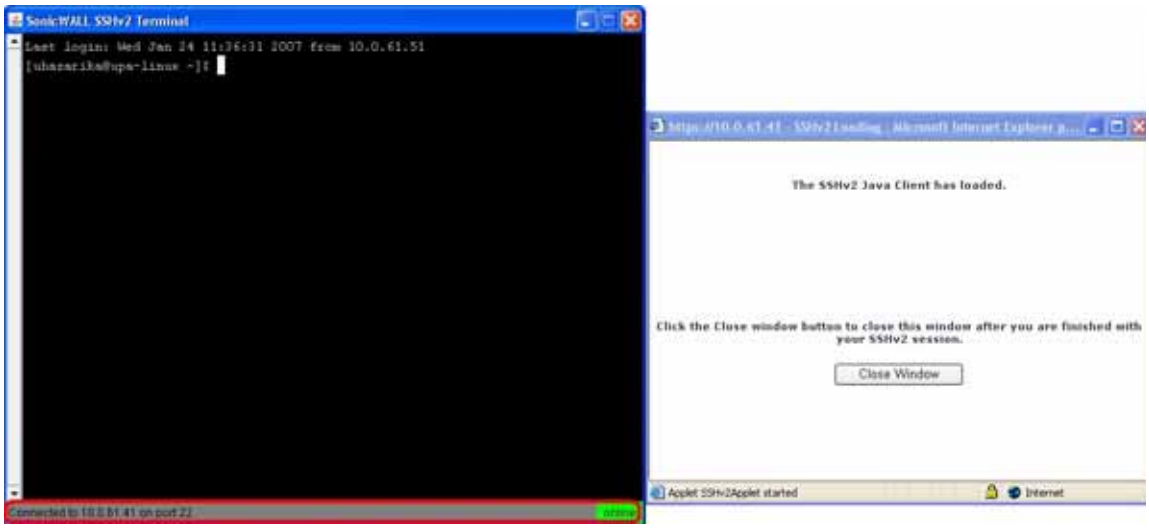
Step 2 A hostkey popup displays. Click **Yes** to accept and proceed with the login process.



Step 3 Enter your password and click **OK**.



Step 4 The SSH terminal launches in a new screen.


SonicWALL SSHv2 Terminal
Last login: Wed Jan 24 11:36:31 2007 from 10.0.61.51
The SSHv2 Java Client has loaded.
Click the Close window button to close this window after you are finished with your SSHv2 session.
Close Window
Applet SSHv2Applet started
Internet

Using HTTP and HTTPS Bookmarks

Note HTTP bookmarks can have a port designation and a path.

Step 1 Click on the HTTP or HTTPS bookmark.

Step 2 A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.

Note OWA Premium, Lotus Domino Web Access and Sharepoint Services are supported in SSL VPN release 3.5. Other applications may work but there may be problems accessing pages that are malformed, have advanced HTML features, use an unsupported authentication method (for example, Windows Integrated Authentication) and URLs that are embedded in Macromedia Flash, Java or ActiveX.

Using File Share Bookmarks

For information on using File Share bookmarks, see the "Using HTML-Based File Shares" section on page 84.

Using Citrix Bookmarks

Citrix is a remote access, application sharing service, similar to RDP. It enables users to remotely access files and applications on a central computer over a secure connection.

Note The Citrix Web Interface feature is supported on the SonicWALL SSL-VPN 2000, SSL-VPN 4000, and SRA 4200 security appliances.

Step 1 Click on the Citrix bookmark.

Step 2 The first time you use a Citrix bookmark, it will install the Citrix Web Client on your computer if you do not already have it.

Click **Install** to install the client.

Internet Explorer - Security Warning
Do you want to install this software?
Name: Citrix Web Client
Publisher: Citrix Systems, Inc
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Step 3 The Citrix Web Client begins to install. If prompted, click the banner to grant ActiveX control to the Citrix Web Client.

https://10.0.61.150 - Citrix Installation - Microsoft Internet Explorer
This site might require the following ActiveX control: 'Citrix Web Client' from 'Citrix Systems, Inc'. Click here to install...
Please wait while the Citrix Web Client is installed ...
After installation, you will be automatically redirected to the Citrix portal

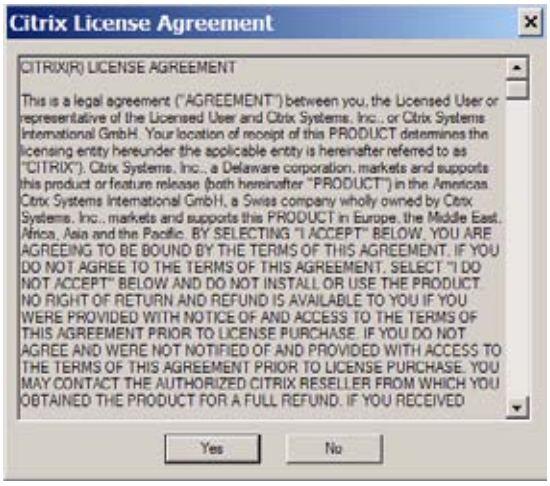
Step 4 Click **Yes** to the Security Warning message that is displayed.

Security Warning
Do you want to install and run "Citrix Web Client" signed on 2/20/2004 10:22 PM and distributed by:
Citrix Systems, Inc
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: Citrix Systems, Inc asserts that this content is safe. You should only install/view this content if you trust Citrix Systems, Inc to make that assertion.
Always trust content from Citrix Systems, Inc
Yes
No
More Info

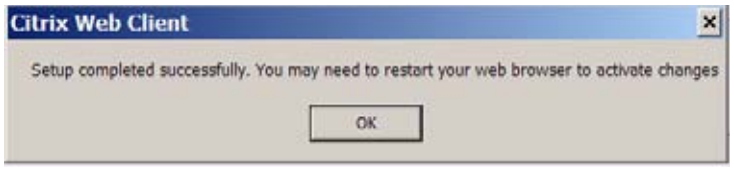
Step 5 The Citrix Web Client installs.

Citrix Web Client - InstallShield Wizard
Extracting Files
The contents of this package are being extracted.
Please wait while the InstallShield Wizard extracts the files needed to install Citrix Web Client on your computer. This may take a few moments.
Extracting wfcrunJ2.exe...
InstallShield
< Back
Next >
Cancel

Step 6 Click **Yes** to the Citrix license agreement.


Citrix License Agreement
CITRIX(R) LICENSE AGREEMENT
This is a legal agreement ("AGREEMENT") between you, the Licensed User or representative of the Licensed User and Citrix Systems, Inc., or Citrix Systems International GmbH. Your location of receipt of this PRODUCT determines the licensing entity hereunder the applicable entity is hereinafter referred to as "CITRIX". Citrix Systems, Inc., a Delaware corporation, markets and supports this product or feature release (both hereinafter "PRODUCT") in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., markets and supports this PRODUCT in Europe, the Middle East, Africa, Asia and the Pacific. BY SELECTING "I ACCEPT" BELOW, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, SELECT "I DO NOT ACCEPT" BELOW AND DO NOT INSTALL OR USE THE PRODUCT. NO RIGHT OF RETURN AND REFUND IS AVAILABLE TO YOU IF YOU WERE PROVIDED WITH NOTICE OF AND ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE. IF YOU DO NOT AGREE AND WERE NOT NOTIFIED OF AND PROVIDED WITH ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE, YOU MAY CONTACT THE AUTHORIZED CITRIX RESELLER FROM WHICH YOU OBTAINED THE PRODUCT FOR A FULL REFUND. IF YOU RECEIVED
Yes
No

Step 7 When the Citrix Web Client has installed, click **OK** If the Citrix Web Interface login window does not display, restart your Web browser and launch the Citrix bookmark again.



Step 8 Enter your username, password, and domain in the Citrix Web Interface login window.

CITRIX
Web Interface
for MetaFrame® Presentation Server
Log in
User name:
Password:
Domain:
Advanced Options >>>
Log In
Welcome
Please log in
To log in to MetaFrame Presentation Server, enter the credentials required, and then click Log In.
If you do not know your log in information, please contact your help desk or system administrator.
Message Center
The Message Center displays any information or error messages that may occur.

Step 9 The Citrix Web Interface home page is displayed. Click on the application you want to use.

Step 10 You may be prompted to install additional Citrix software.

Security Warning
Do you want to install and run "https://10.0.61.150/XTSAC.cab" signed on an unknown date/time and distributed by:
SonicWALL, Inc.
Publisher authenticity verified by Thawte Code Signing CA
Caution: SonicWALL, Inc. asserts that this content is safe. You should only install/view this content if you trust SonicWALL, Inc. to make that assertion.
Always trust content from SonicWALL, Inc.
Yes
No
More Info

Step 11 The shared application is now launched.

Global Bookmark Single Sign-On Options

You can configure single sign-on using the **Options** button on the main Virtual Office page. SSO settings will be enabled only if the administrator has configured user- controlled single sign-on (SSO). To configure SSO bookmark options, perform the following tasks:

Step 1 Click the **Options** button at the top right of the Virtual Office. The **User Options** page displays.

SONICWALL Virtual Office
User: jpollock
Session Status: Active
Options
Help
Logout
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network
Virtual Assist
Assist someone by taking control of their computer.
Tips/Help
Search Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.

Step 2 Under **Single Sign-On Settings**, select **Use SSL VPN account credentials to log into bookmarks** to enable SSO for bookmarks. Leave the box unchecked if you do not want to use SSO for bookmarks.

Step 3 Click **Save** to save your changes.

Note Fileshares will use the configured domain name of which the user is a member to supply to the backend server. HTTP, HTTPS, FTP, RDP - ActiveX, RDP- Java will supply the username and password that was used to login. If the server is expecting a domain-prefixed username, SSO will fail. In some cases, a default domain can be specified at the server to allow SSO to succeed.

Per-Bookmark Single Sign-On Options

SonicWALL SSL VPN supports per-bookmark single sign-on for the following bookmark services:

- Terminal Services (RDP - Active X)
- Terminal Services (RDP - Java)
- FTP

Per-Bookmark SSO allows users to enable or disable SSO for individual bookmarks. This flexibility in specifying login credentials is useful in the following cases:

- Users who use multiple accounts to access a variety of resources.
- Users who use two-factor authentication to log in to the SSL VPN Virtual Office, but use a static password to access other resources.
- Users who need to access servers that require a domain prefix.

To configure per-bookmark SSO, perform the following tasks.

Step 1 Before enabling SSO on an individual bookmark, you must first enable SSO globally as described in the "Global Bookmark Single Sign-On Options" section on page 108.

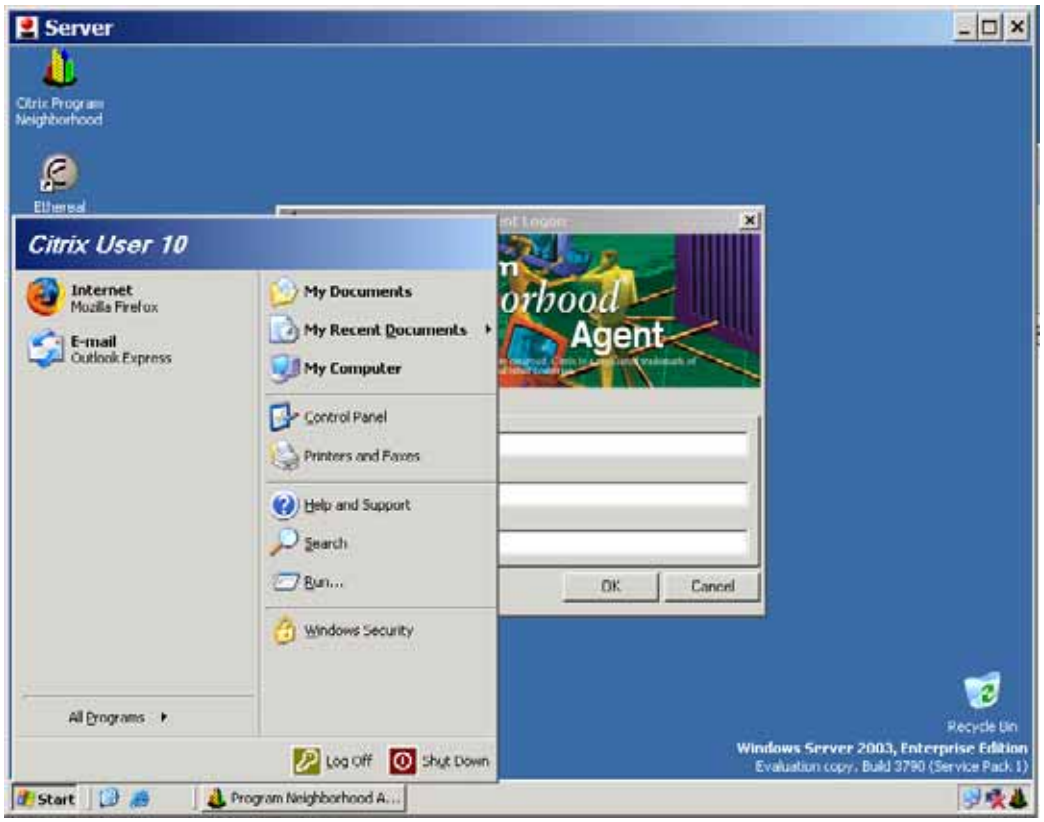
Step 2 On the Virtual Office page, click on the **Add Bookmark** button.

Step 3 Select one of the service types that supports per-bookmark SSO: **Terminal Services (RDP - Active X)**, **Terminal Services (RDP - Java)**, or **FTP**.

Step 4 To use SSO for the bookmark, ensure that the **Automatically log in** checkbox is checked and select the **Use SSL VPN account credentials** radio button.

Step 5 To disable SSO for the bookmark, ensure that the **Automatically log in** checkbox is selected and then select the **Use custom credentials** radio button.

Step 6 Enter the **User name** and **password** for the service.



Logging Out of the Virtual Office

To end your session, simply return to the Virtual Office home page from wherever you are within the portal and click on the Logout button.

SONICWALL Virtual Office
User: jpollock
Session Status: Active
Options
Help
Logout
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate
Virtual Assist
Assist someone by taking control of their
Tips/Help
Search Help
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote

Logout

Note When using the Virtual Office with the **admin** username, the **Logout** button is not displayed. This is a security measure to ensure that administrators log out of the administrative interface, and not the Virtual Office.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

SonicWALL, Inc.

2001 Logic Drive
San Jose, CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-001785-00
Rev A 10/09

©2009 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.